

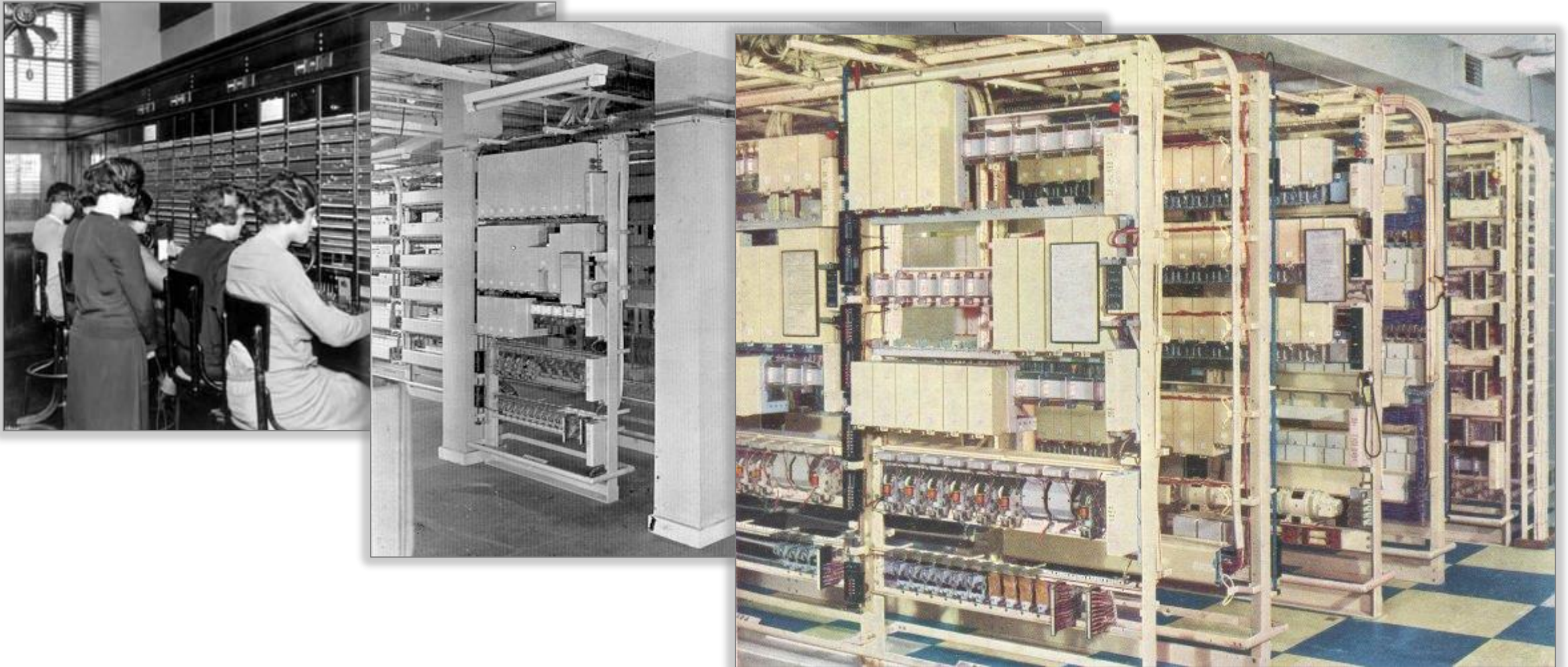
# Attacks on Telecom Operators and Mobile Subscribers via SS7

**Dmitry Kurbatov**

Security specialist

Positive Research

# Yesterday: Closed Ecosystems

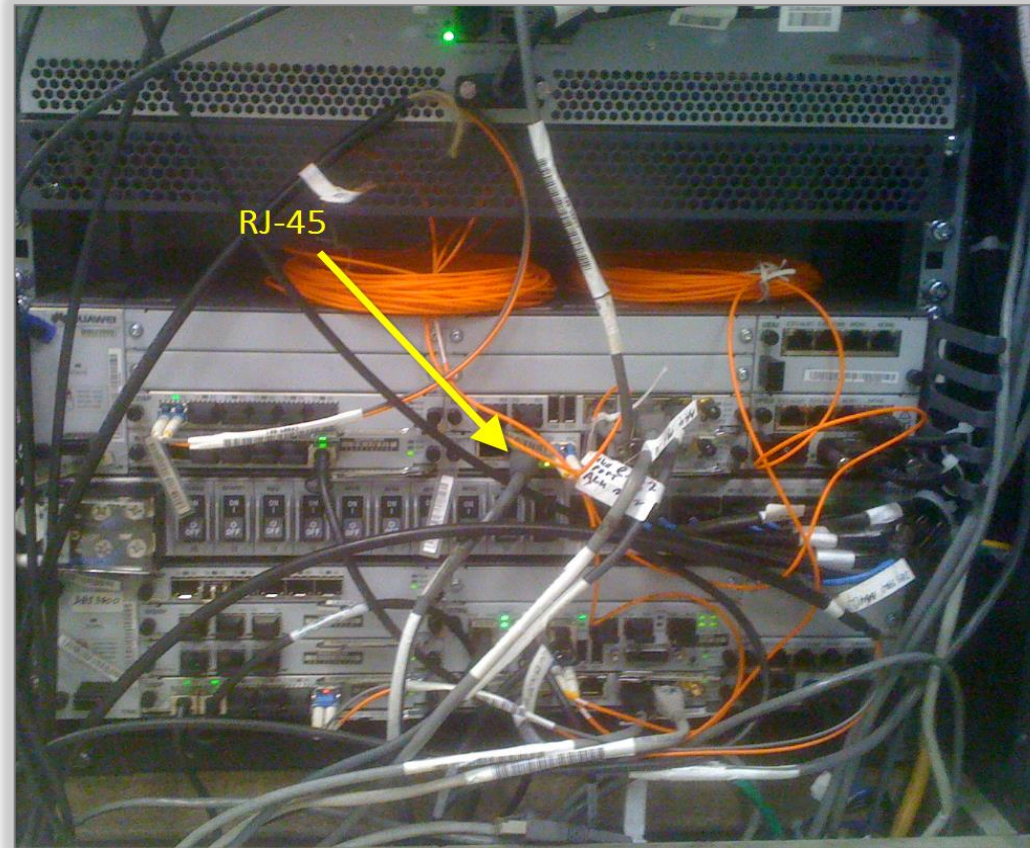


# Today: Unified Technologies





# Today: Common Interfaces



# Today: IP Connectivity

The screenshot shows the Shodan search engine interface. At the top, there is a navigation bar with links to Shodan, Exploits, Scanhub, Maps, Blog, and Membership. On the right side of the navigation bar are links for Register and Login. Below the navigation bar is a search bar with the text 'port:2123' and a 'Search' button. To the right of the search bar, a red box highlights the text 'Results 1 - 6 of about 14779 for port:2123'. Below the search bar, there is a section titled 'Top Countries' with a list of countries and their corresponding counts: Korea, Republic of (6,744), China (3,339), Israel (1,230), Turkey (544), and United States (394). To the right of the 'Top Countries' section, there are three IP address entries. Each entry includes the IP address, the organization name, the date it was added, and a list of details. The first entry is for IP 175.113.123.24, SK Broadband, added on 04.02.2015. The second entry is for IP 121.173.248.253, Korea Telecom, added on 04.02.2015. The third entry is for IP 120.199.138.55, China Mobile, added on 04.02.2015. Each entry has a red box highlighting the text 'GPRS Tunneling Protocol'. Below the 'GPRS Tunneling Protocol' text, there are details for each entry: 'Correct data length for version 1', 'Version: 1', 'Flags: XXX1 0010', 'Type: 2 (Echo response)', 'Length: 6', and 'Data: \x0c=\x00\x00\x0e\x02' for the first entry, 'Data: \x0c=\x00\x00\x0e\x03' for the second entry, and 'Data: \x0c=\x00\x00\x0e\x03' for the third entry.

Shodan Exploits Scanhub Maps Blog Membership Register Login

SHODAN port:2123 Search

Results 1 - 6 of about 14779 for port:2123

**Top Countries**

|                                    |       |
|------------------------------------|-------|
| <a href="#">Korea, Republic of</a> | 6,744 |
| <a href="#">China</a>              | 3,339 |
| <a href="#">Israel</a>             | 1,230 |
| <a href="#">Turkey</a>             | 544   |
| <a href="#">United States</a>      | 394   |

**175.113.123.24**  
SK Broadband  
Added on 04.02.2015

GPRS Tunneling Protocol  
Correct data length for version 1  
Version: 1  
Flags: XXX1 0010  
Type: 2 (Echo response)  
Length: 6  
Data: \x0c=\x00\x00\x0e\x02

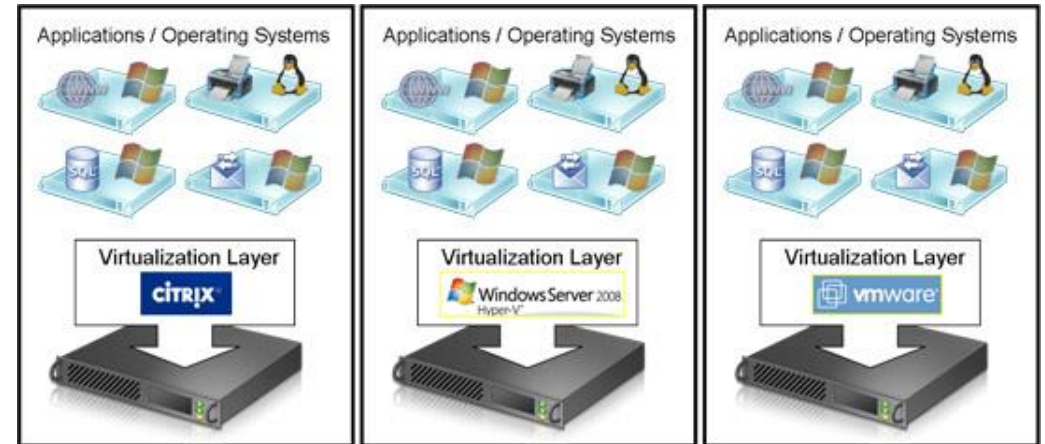
**121.173.248.253**  
Korea Telecom  
Added on 04.02.2015

GPRS Tunneling Protocol  
Correct data length for version 1  
Version: 1  
Flags: XXX1 0010  
Type: 2 (Echo response)  
Length: 6  
Data: \x0c=\x00\x00\x0e\x03

**120.199.138.55**  
China Mobile  
Added on 04.02.2015

GPRS Tunneling Protocol  
Correct data length for version 1

# Tomorrow: virtualization



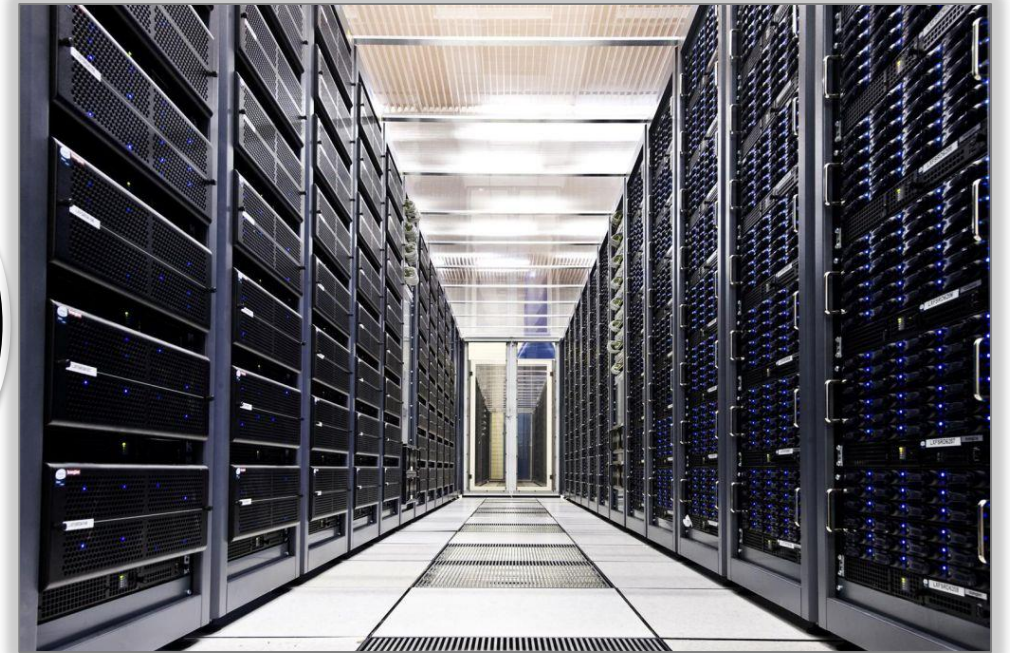


# Time Machine

Through SIGTRAN back to 1970's



SIGTRAN



# 2014 was a good year for SS7 security



## Hackito Ergo Sum 2014

- Locating mobile phones



## Positive Hack Days IV

- How to Intercept a Conversation Held on the Other Side of the Planet

## Washington Post

- Secretly track cellphones

## 31C3

- SS7: Locate. Track. Manipulate
- Mobile self-defense



ΘICΘ

a new dawn

31st Chaos Communication Congress



# Topics

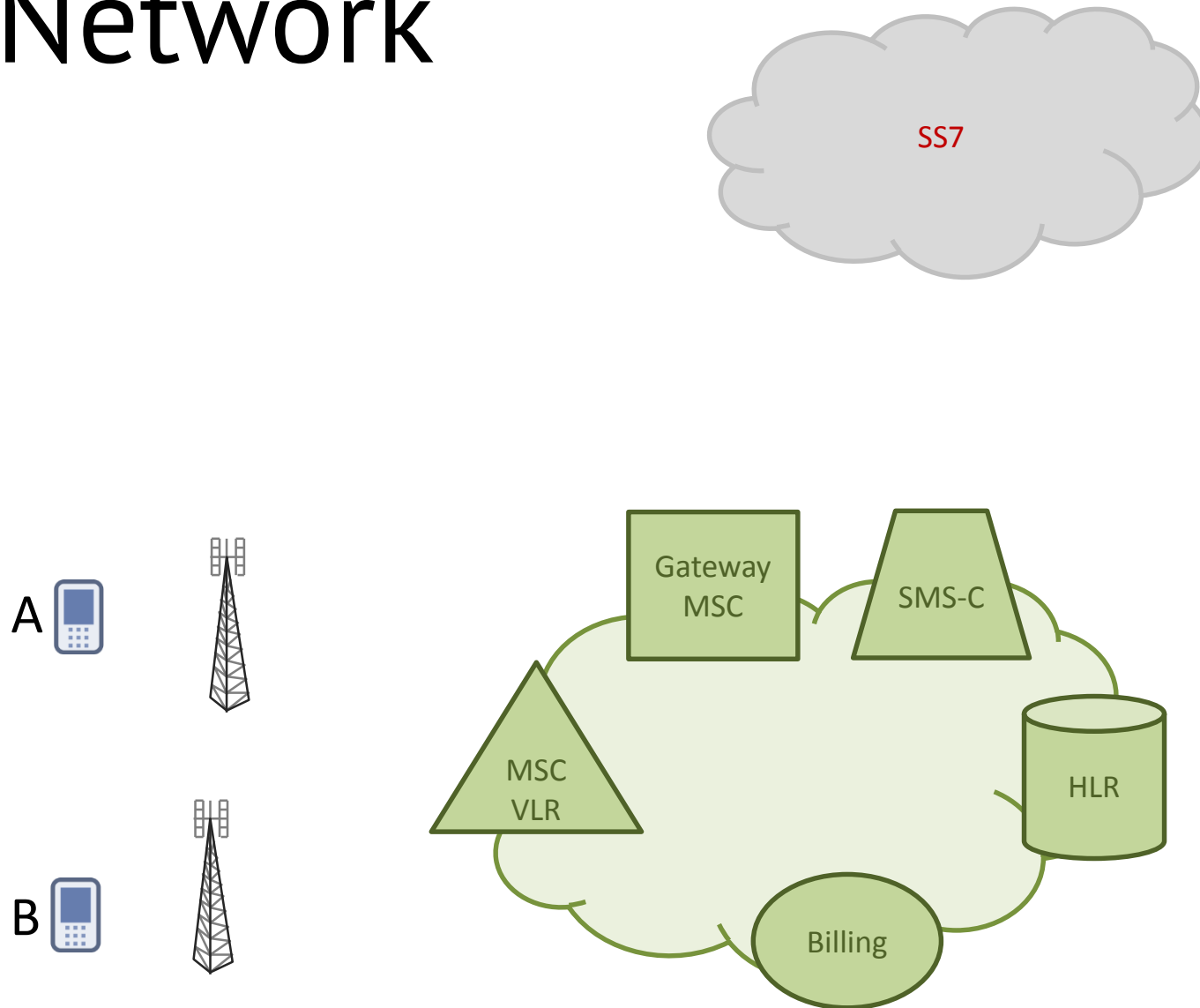
USSD Money Transfer  
Short Message Interception

**Hot for everyone**

DoS on Mobile Switching Center  
Fraud in SS7 network

**Hot for mobile network operators**

# SS7 Network

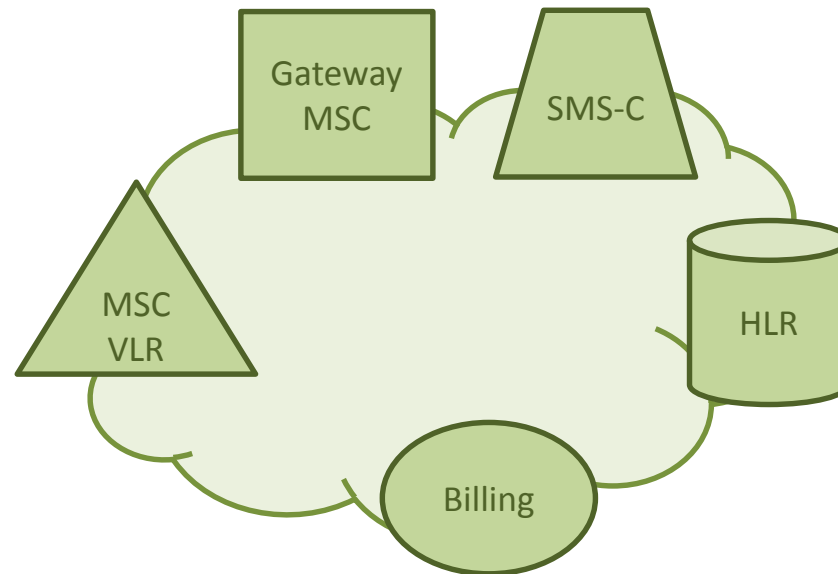
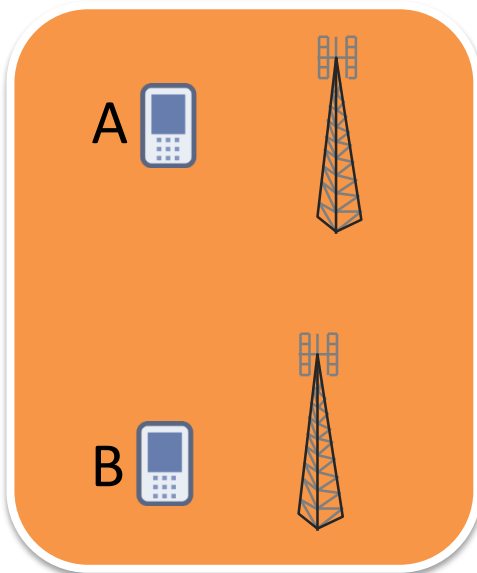


# Radio Part

Cell Phone

Base Transceiver Station

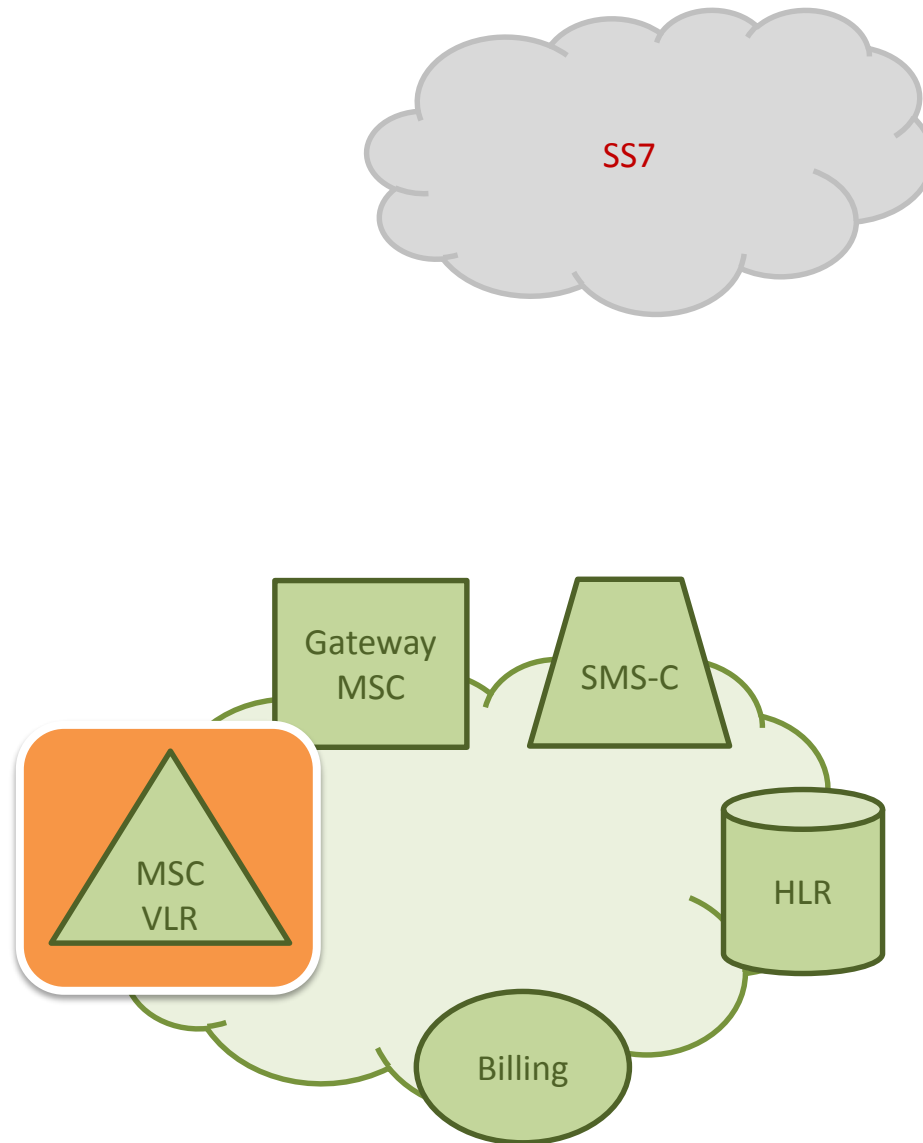
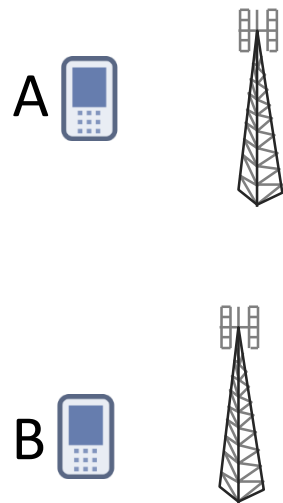
Base Station Controller





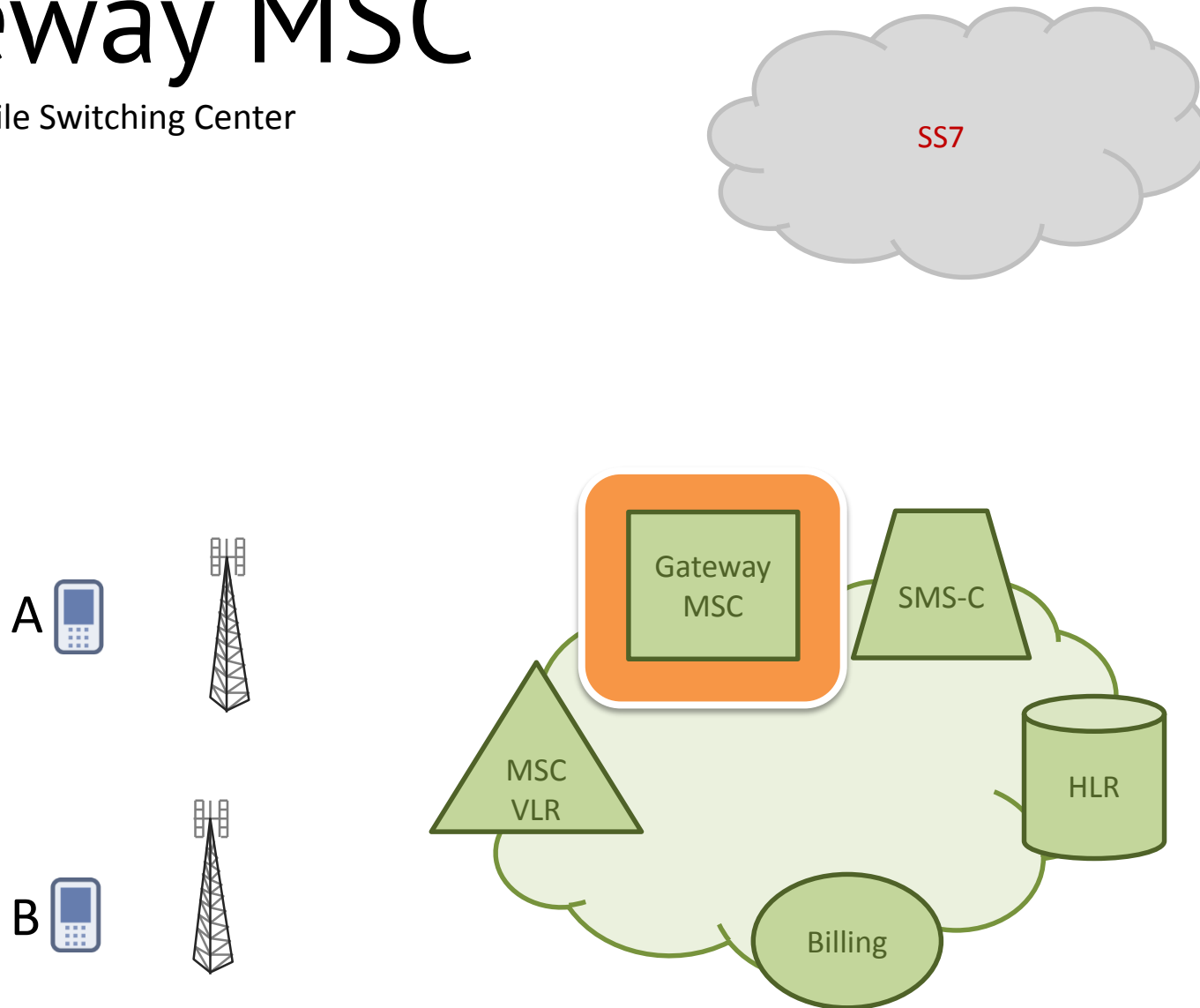
# MSC/VLR

Mobile Switching Center  
Visitor Location Register



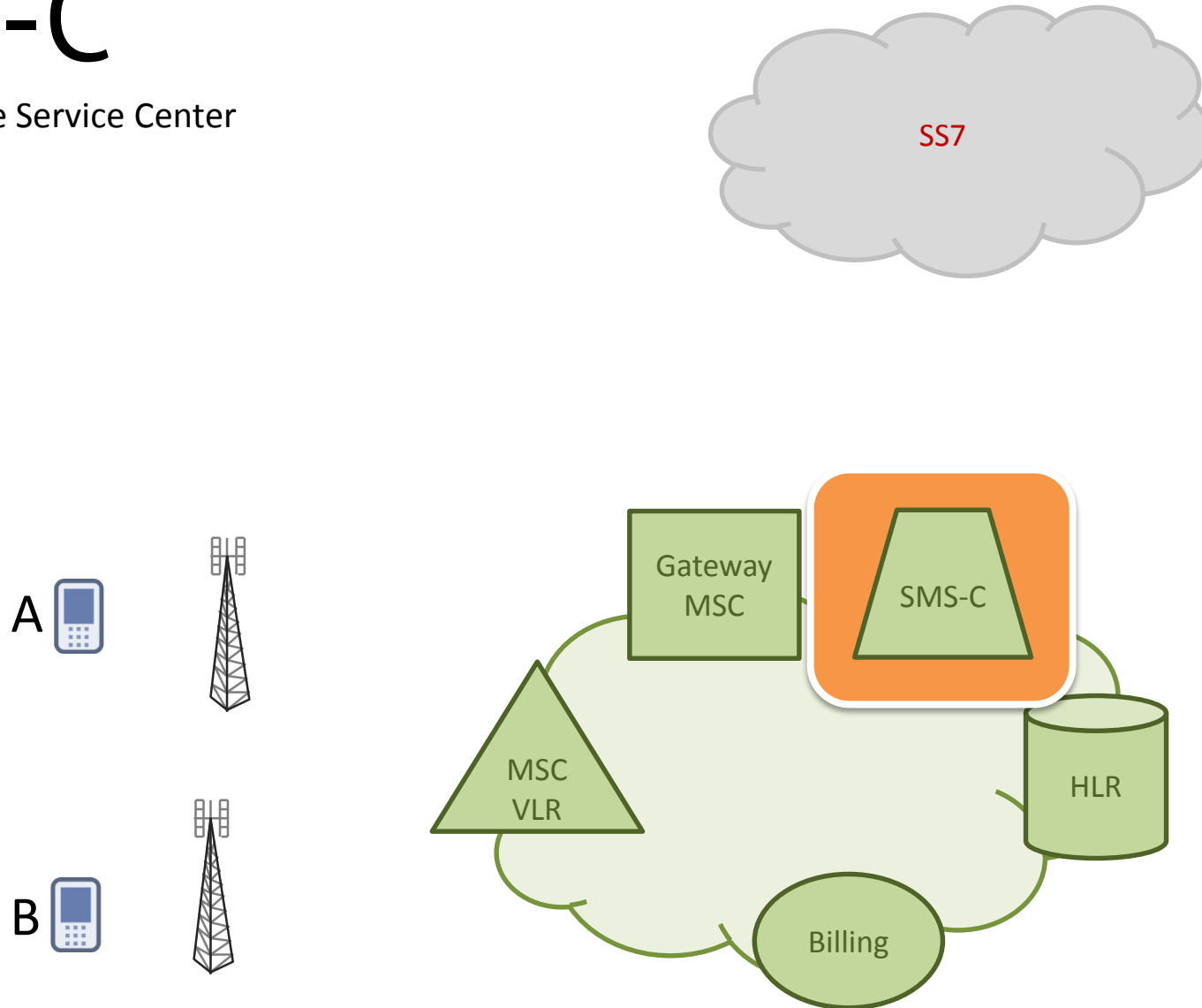
# Gateway MSC

Gateway Mobile Switching Center



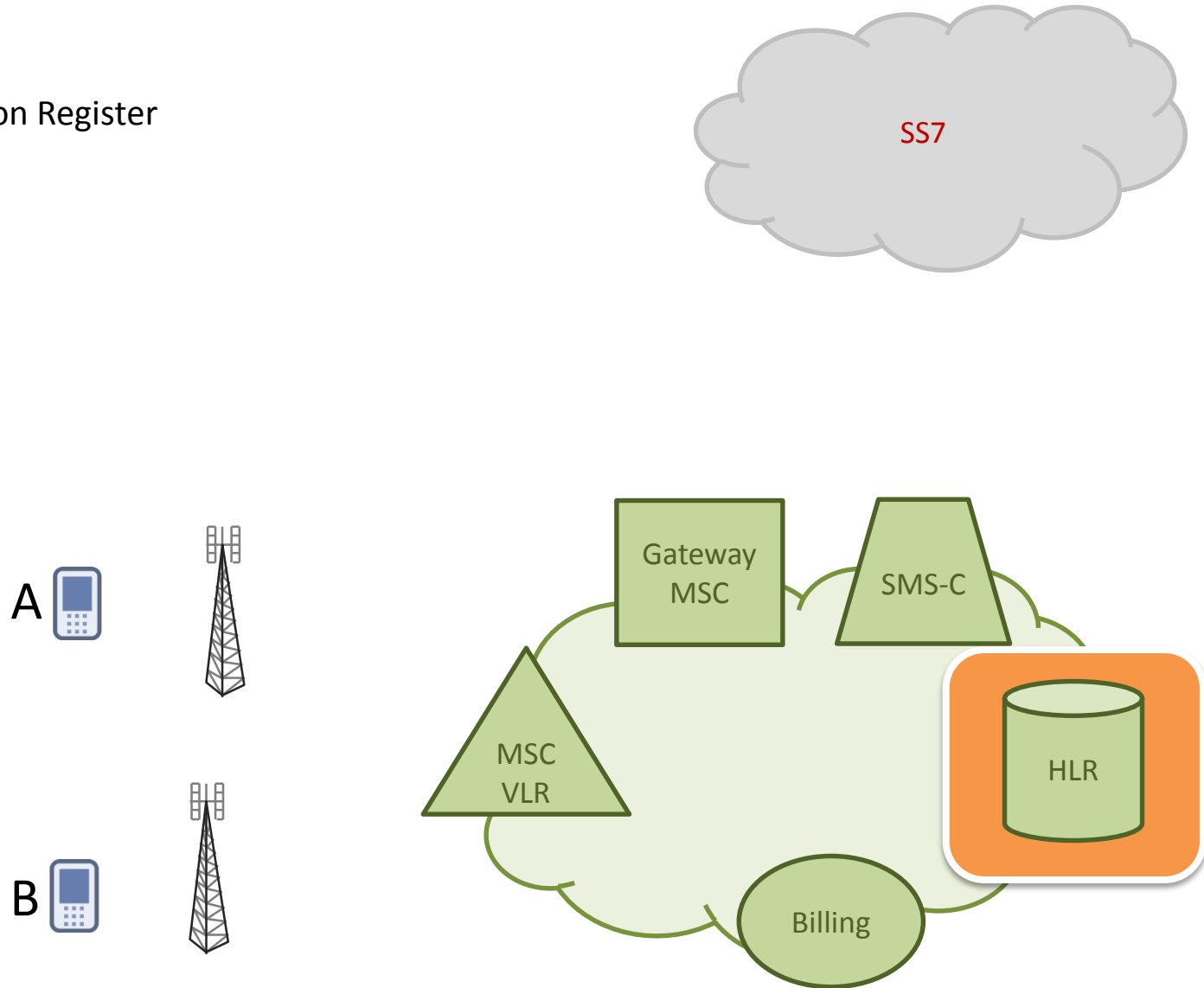
# SMS-C

Short Message Service Center



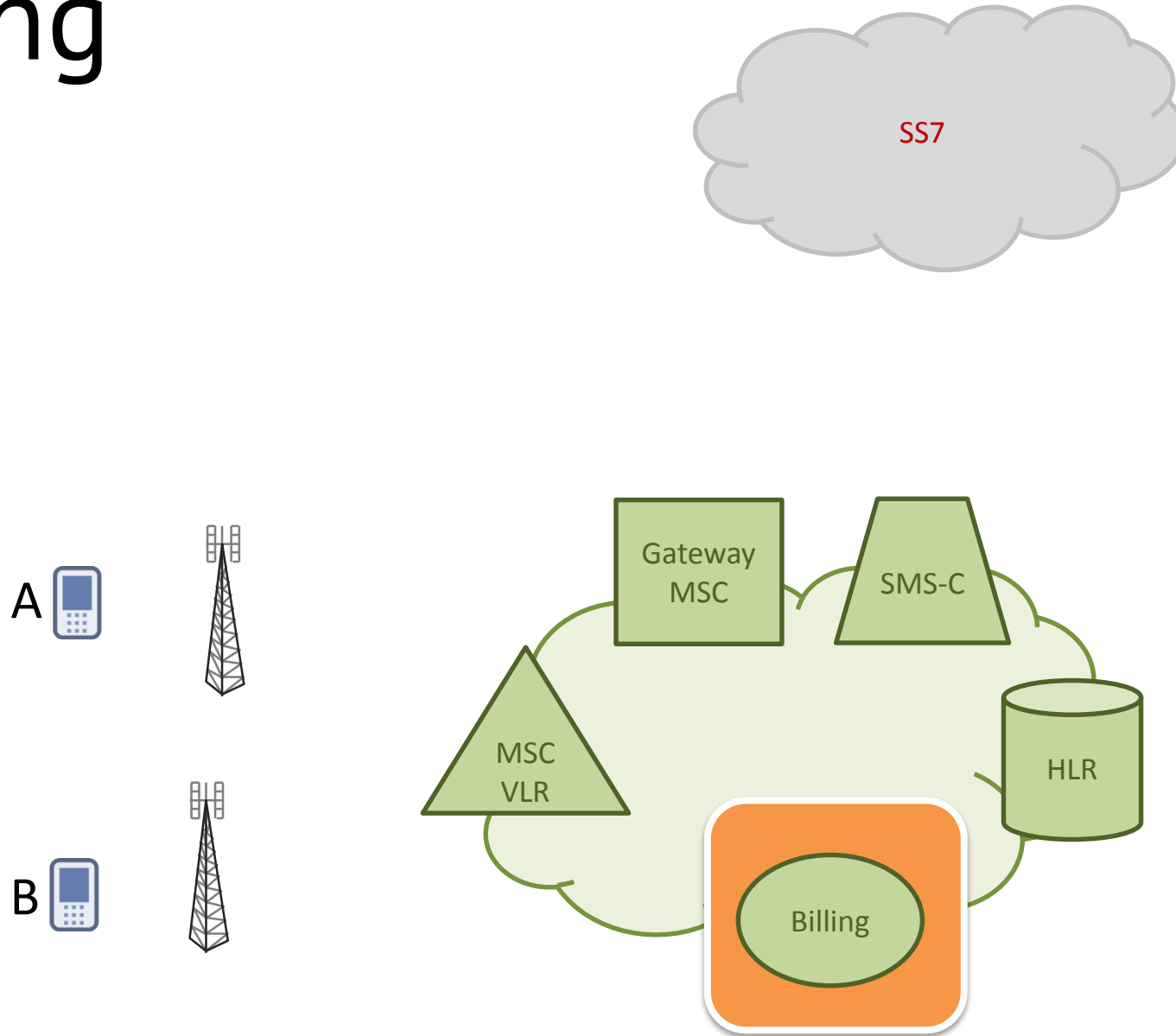
# HLR

Homey Location Register



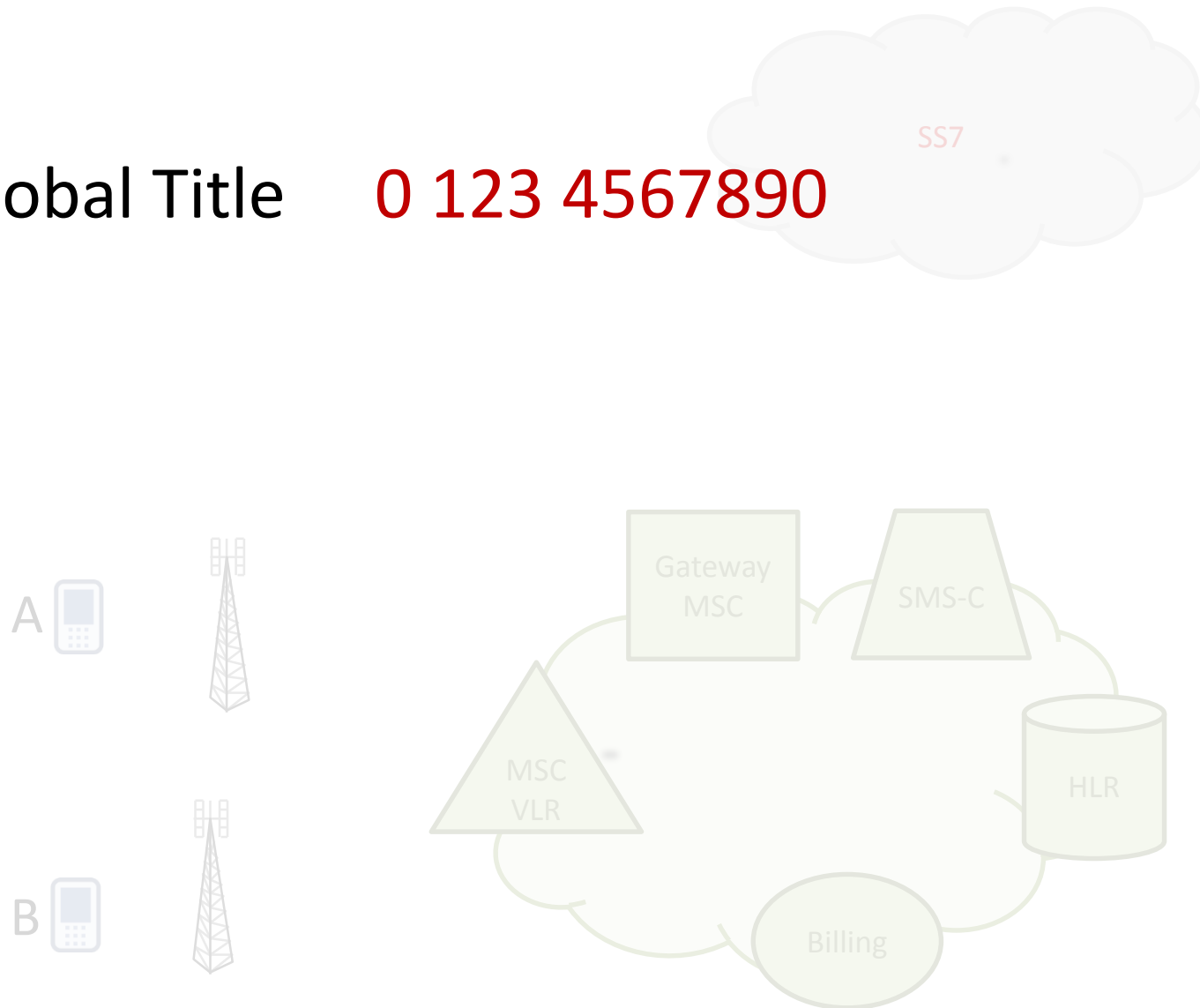


# Billing



# IDs

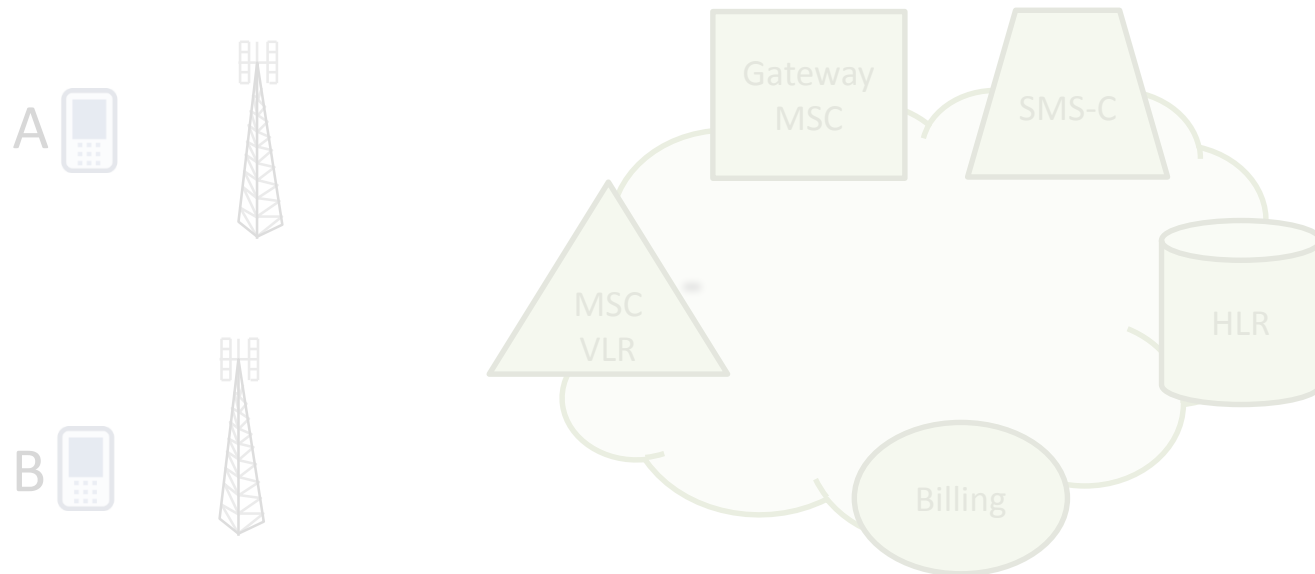
GT – Global Title    0 123 4567890



# IDs

**GT** – Global Title     0 123 4567890

**MSISDN** – A or B mobile numbers     0 123 4567890

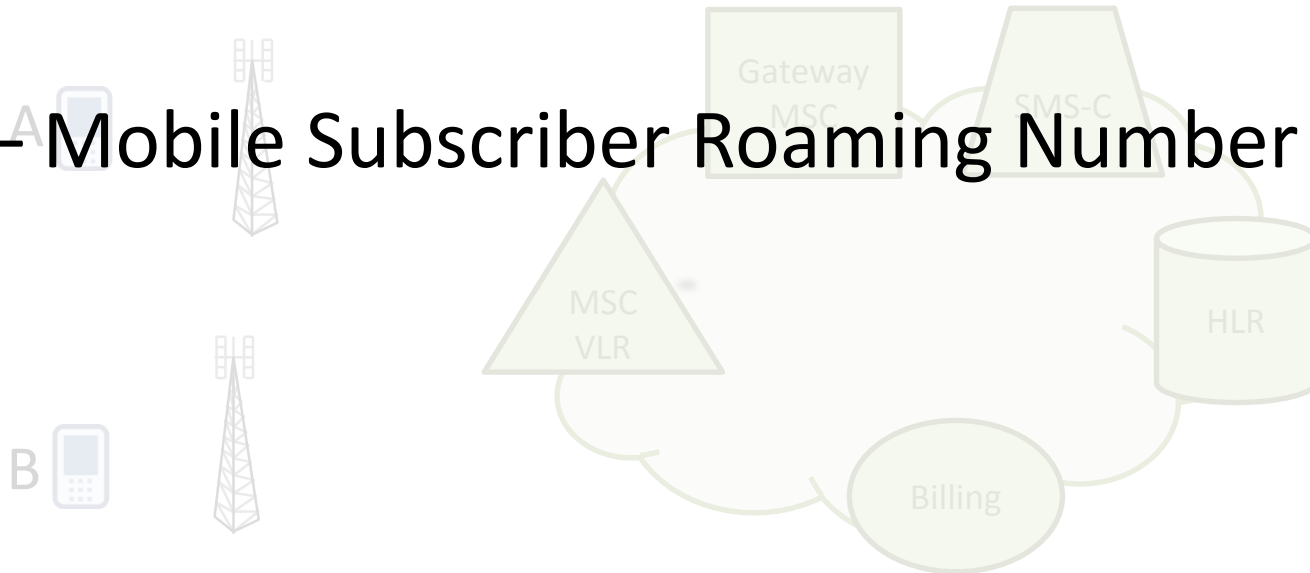


# IDs

**GT** – Global Title    0 123 4567890

**MSISDN** – A or B mobile numbers    0 123 4567890

**MSRN** – Mobile Subscriber Roaming Number    0 123 4567890



# IDs

**GT** – Global Title    0 123 4567890

**MSISDN** – A or B mobile numbers    0 123 4567890

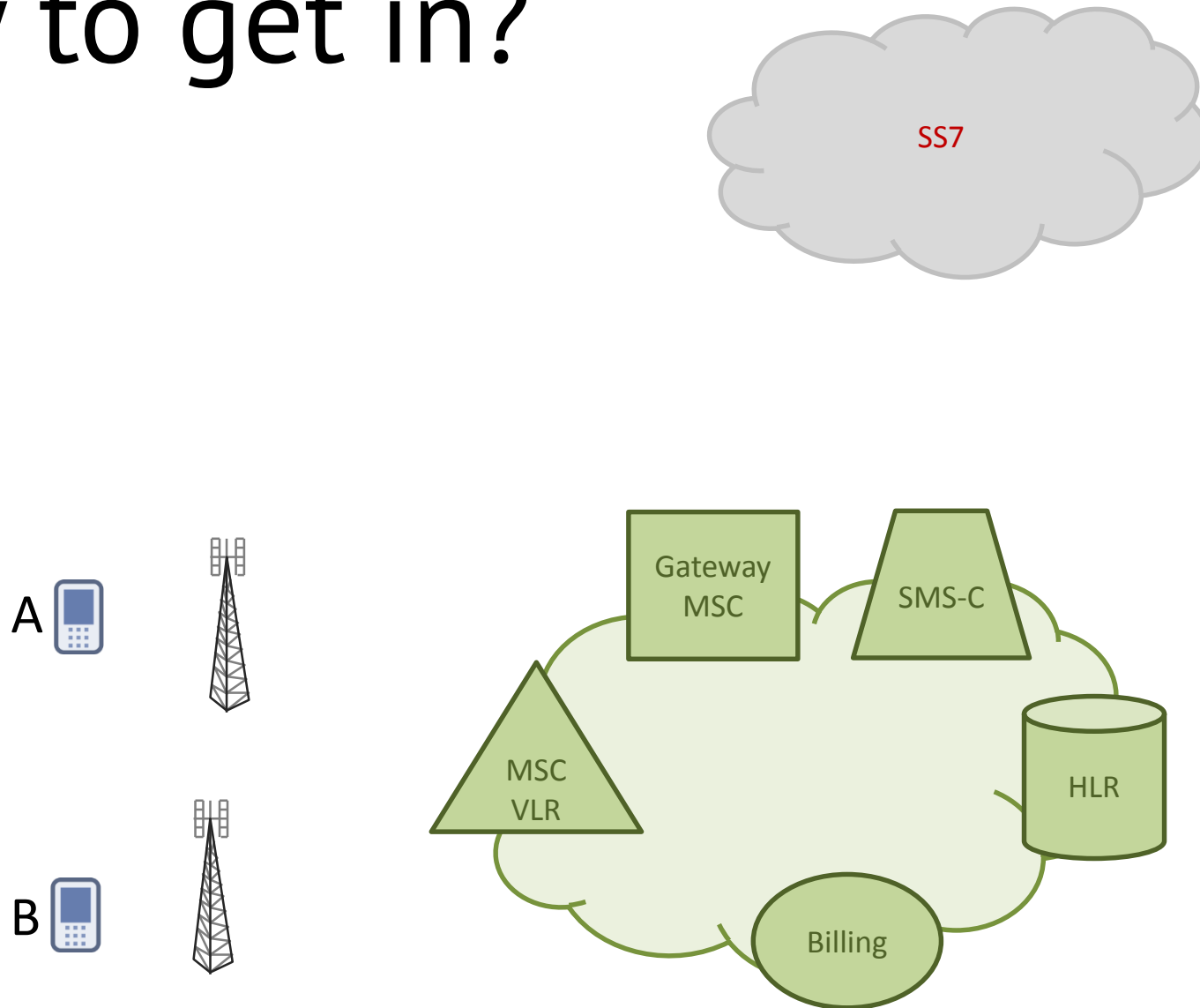
**MSRN** – Mobile Subscriber Roaming Number    0 123 4567890

**IMSI** – International Mobile Subscriber Identity    15 digits

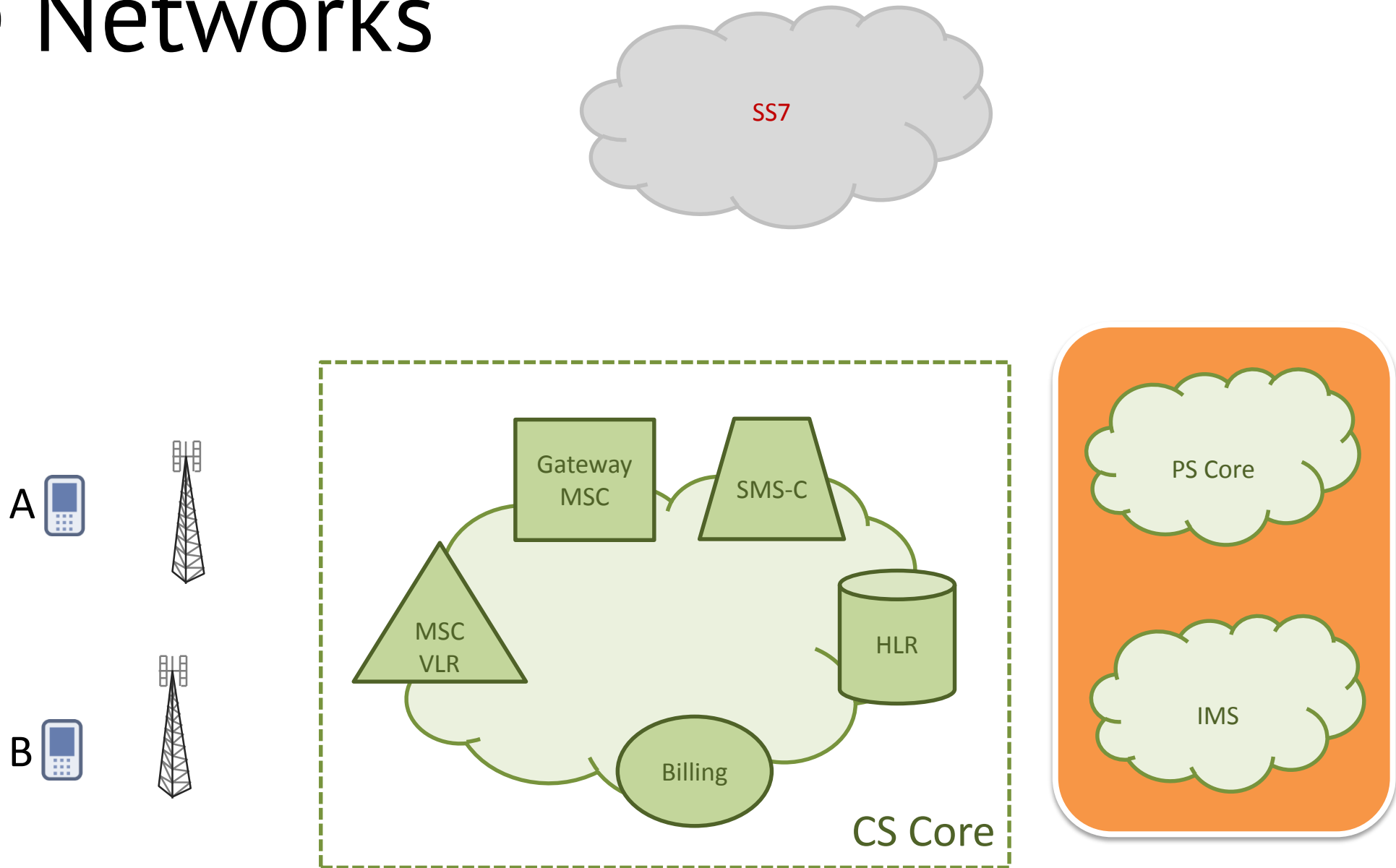




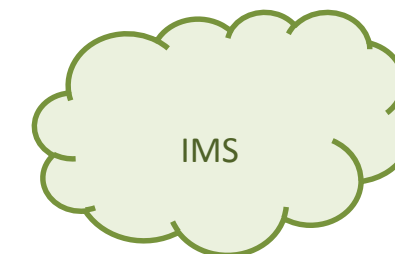
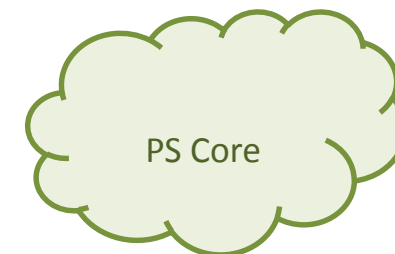
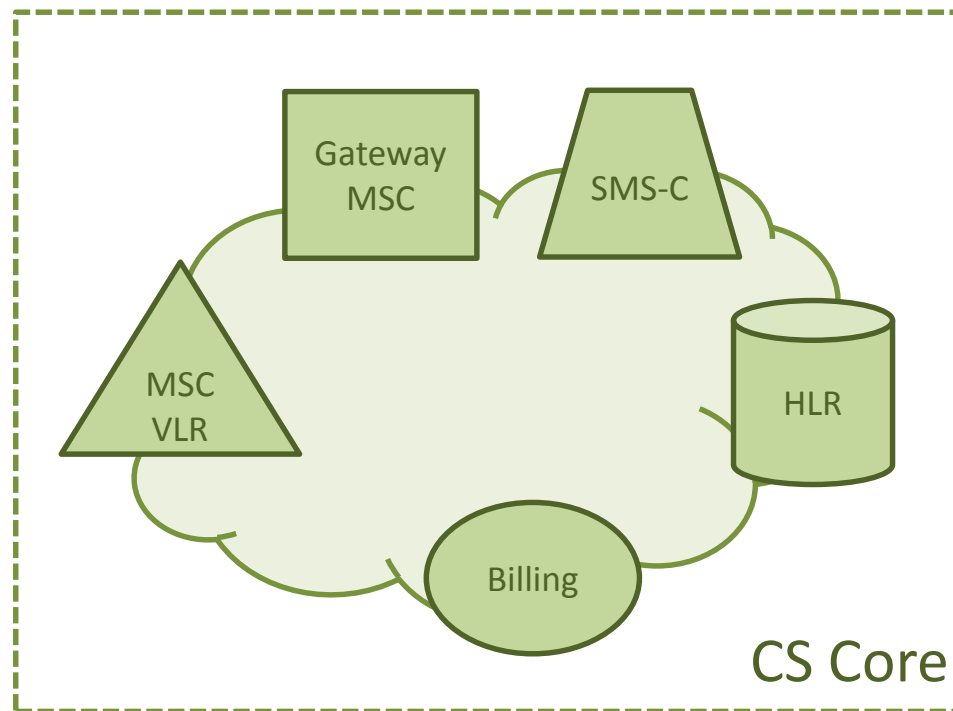
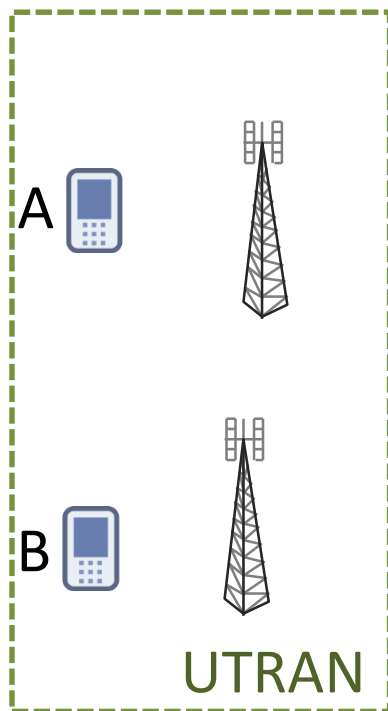
# How to get in?



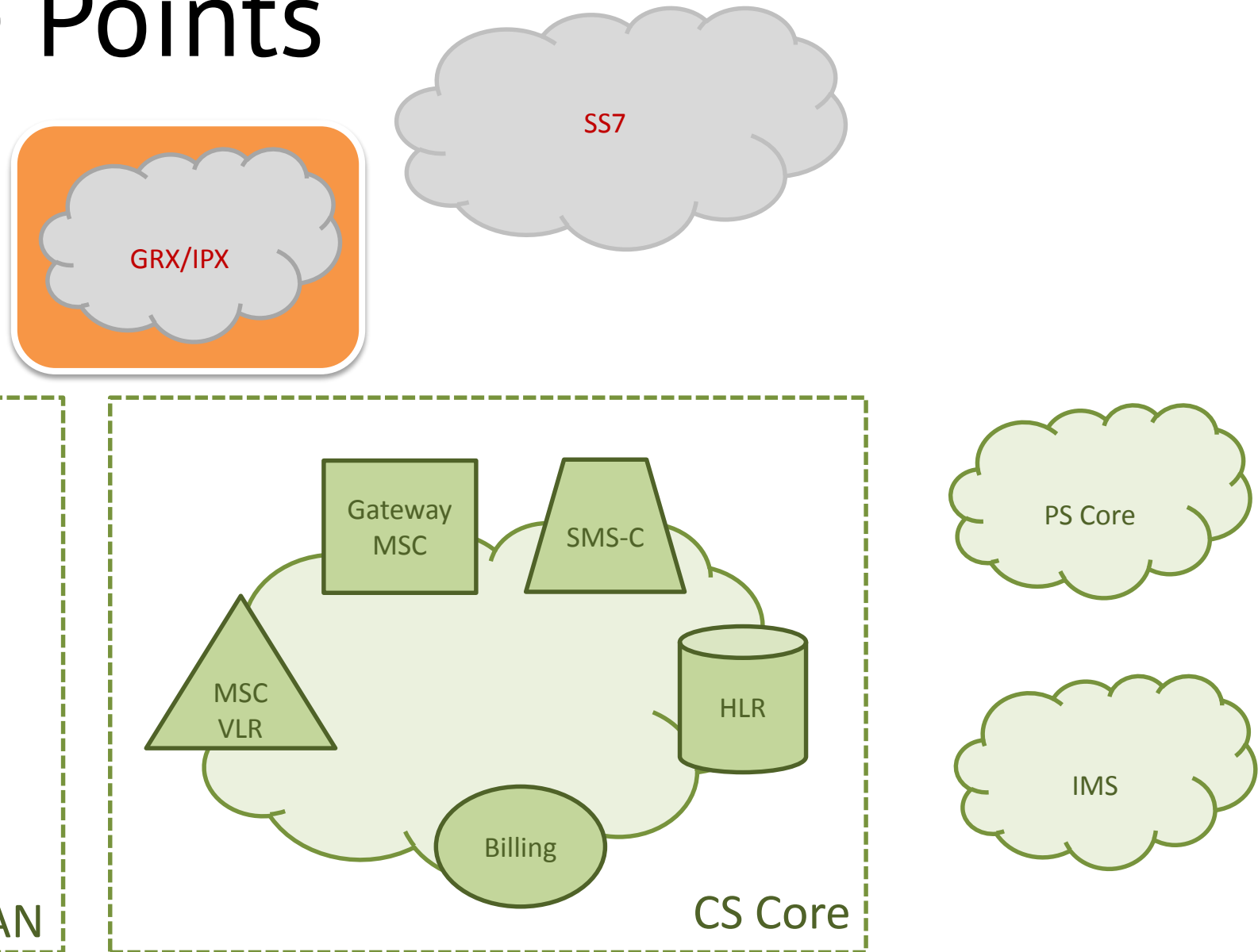
# Core Networks



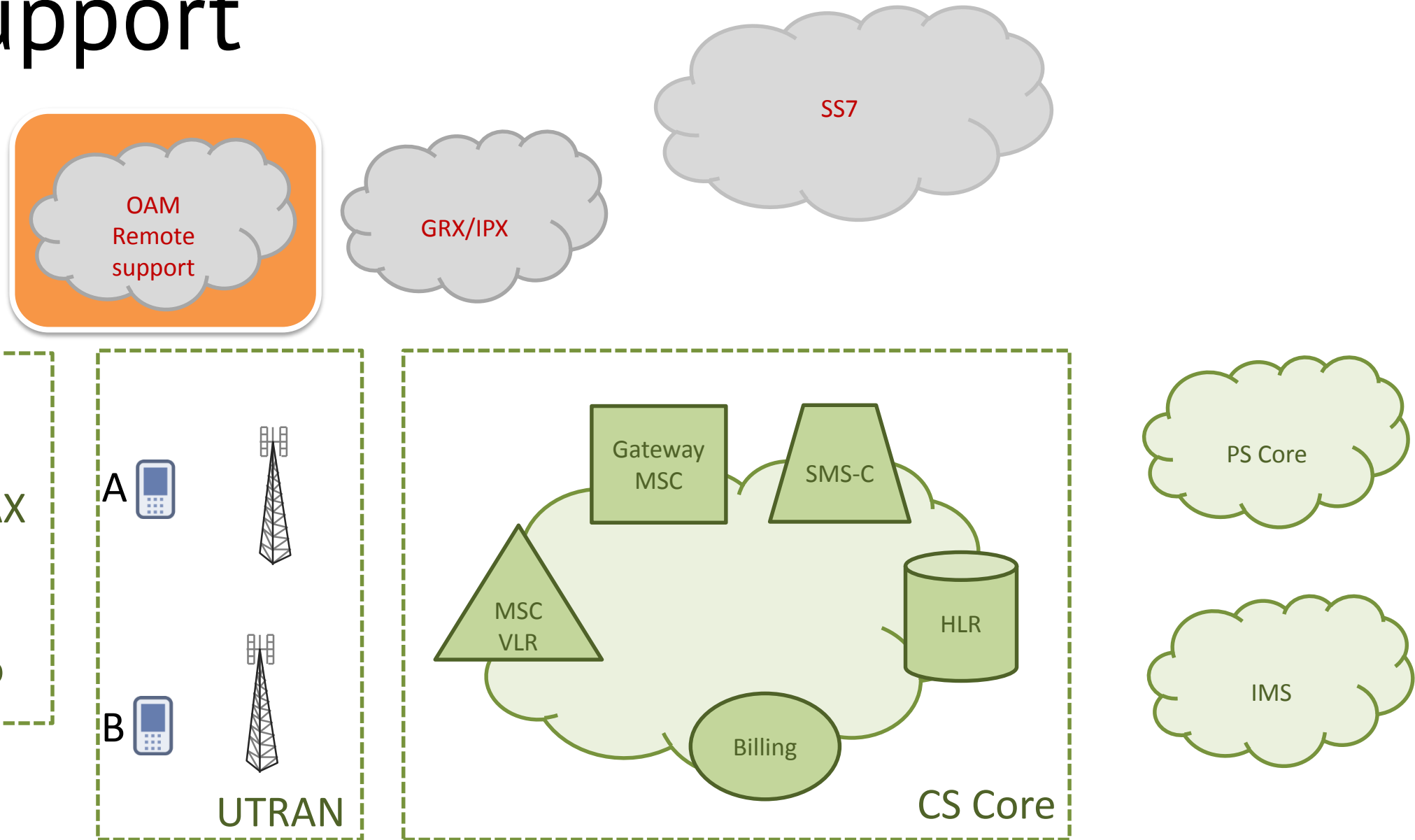
# Access Networks



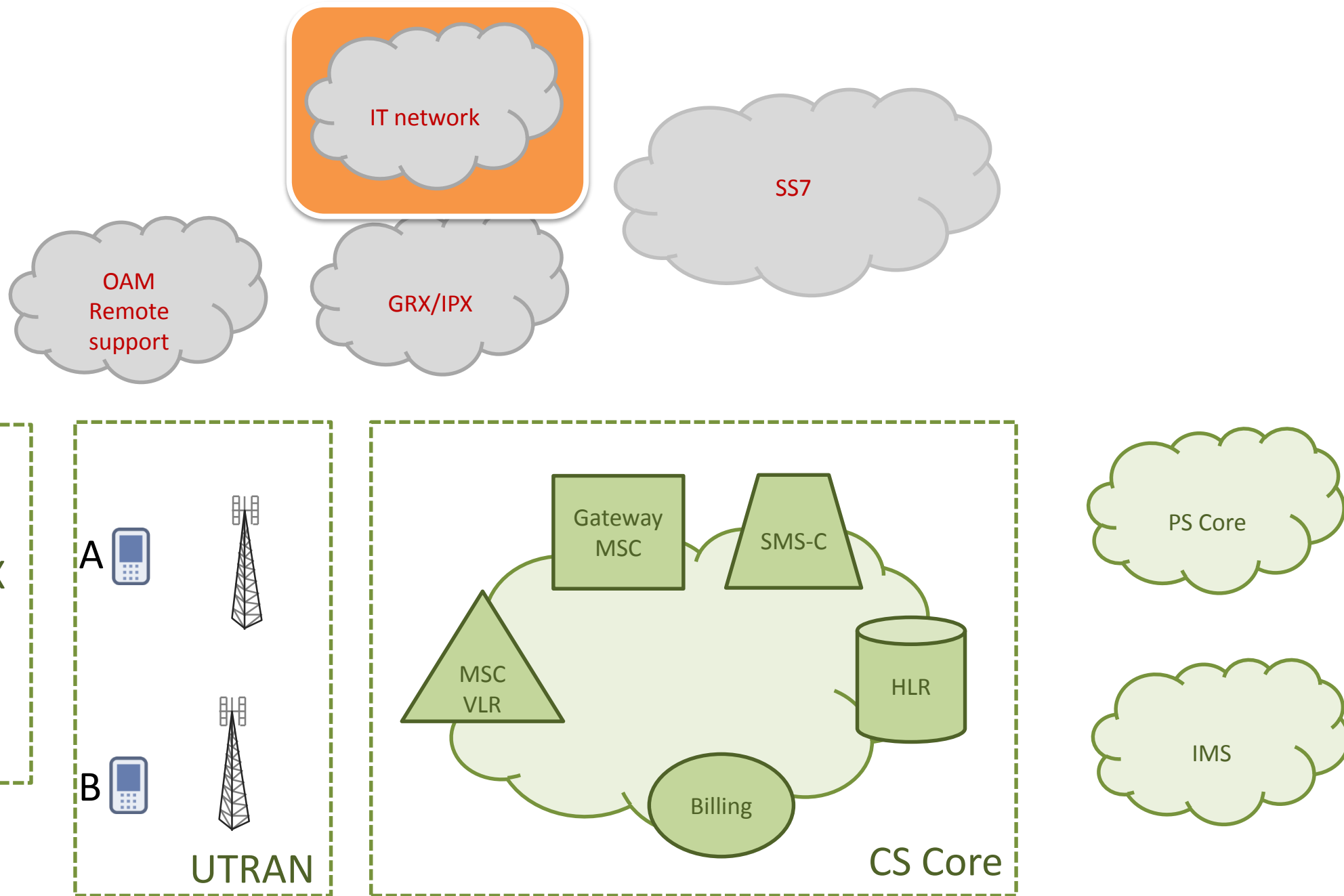
# Exchange Points



# Support

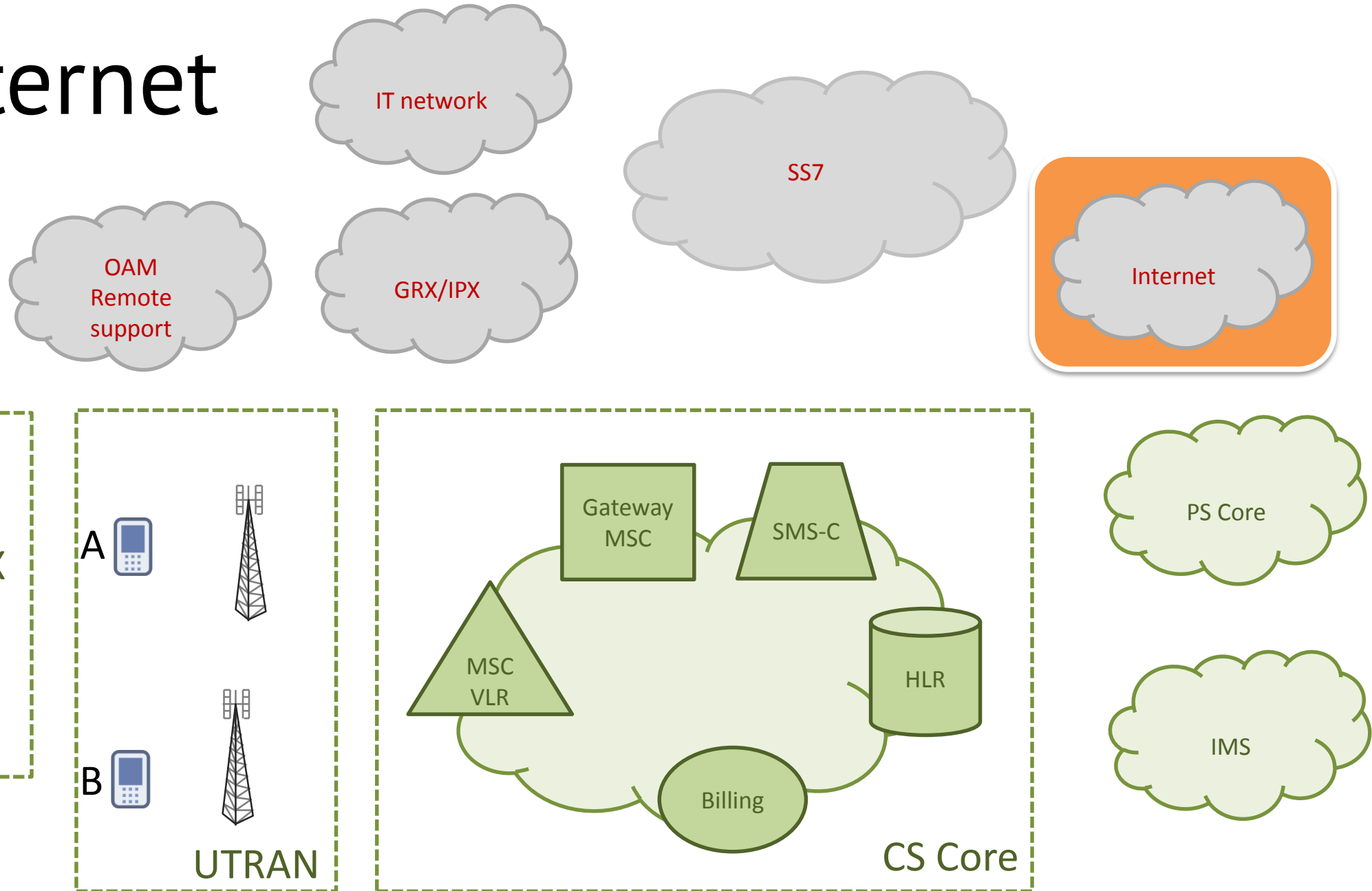


# IT

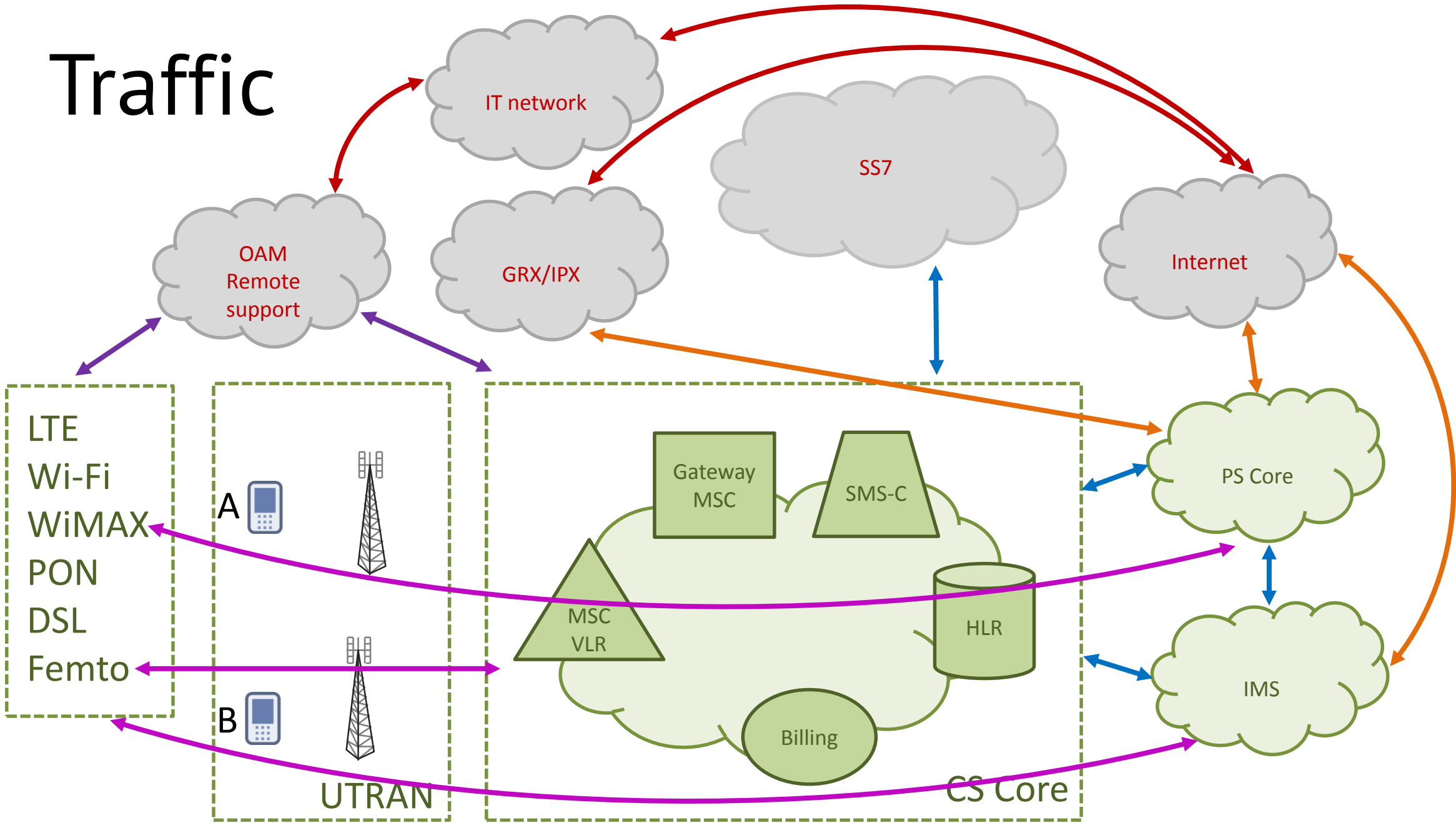




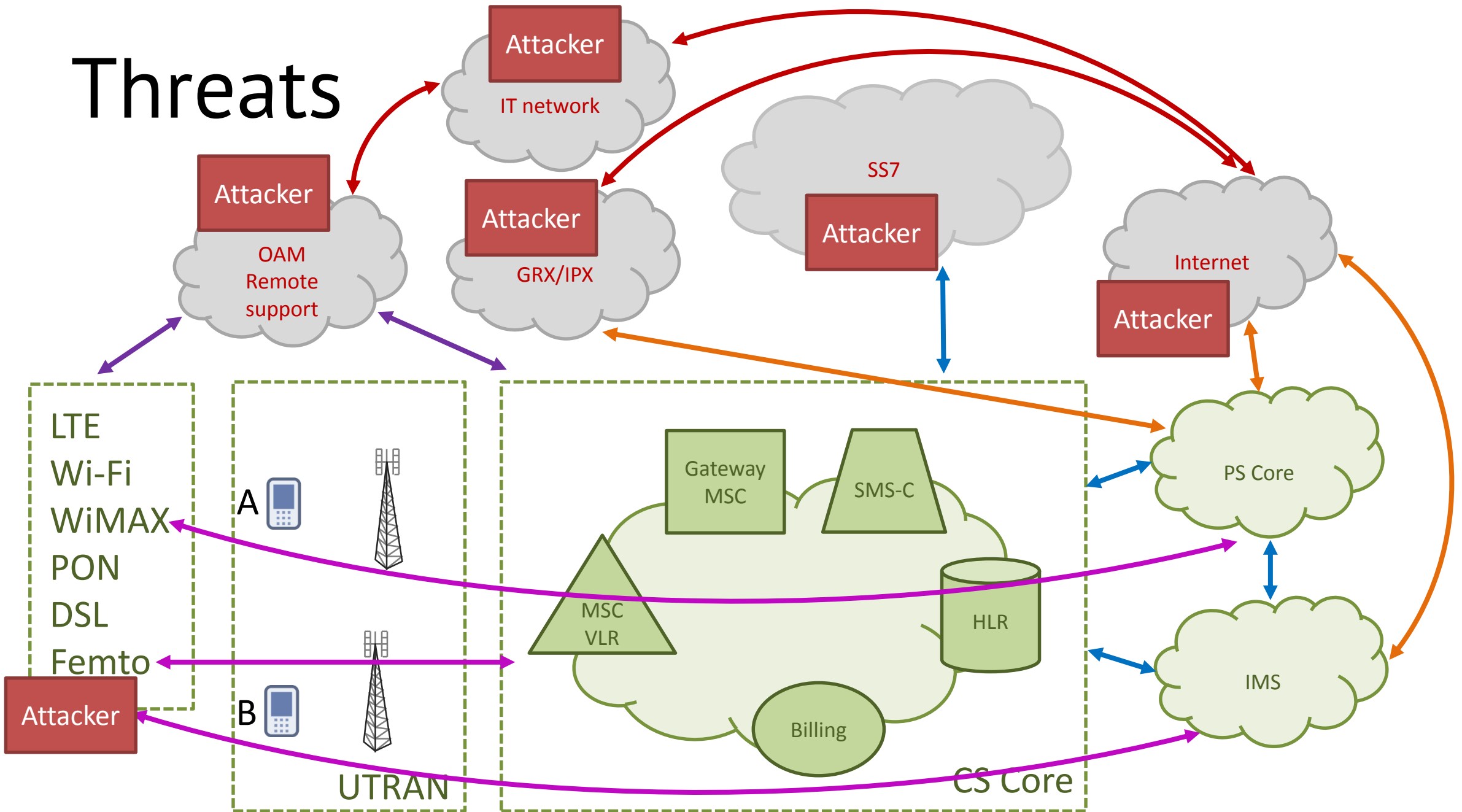
# Internet



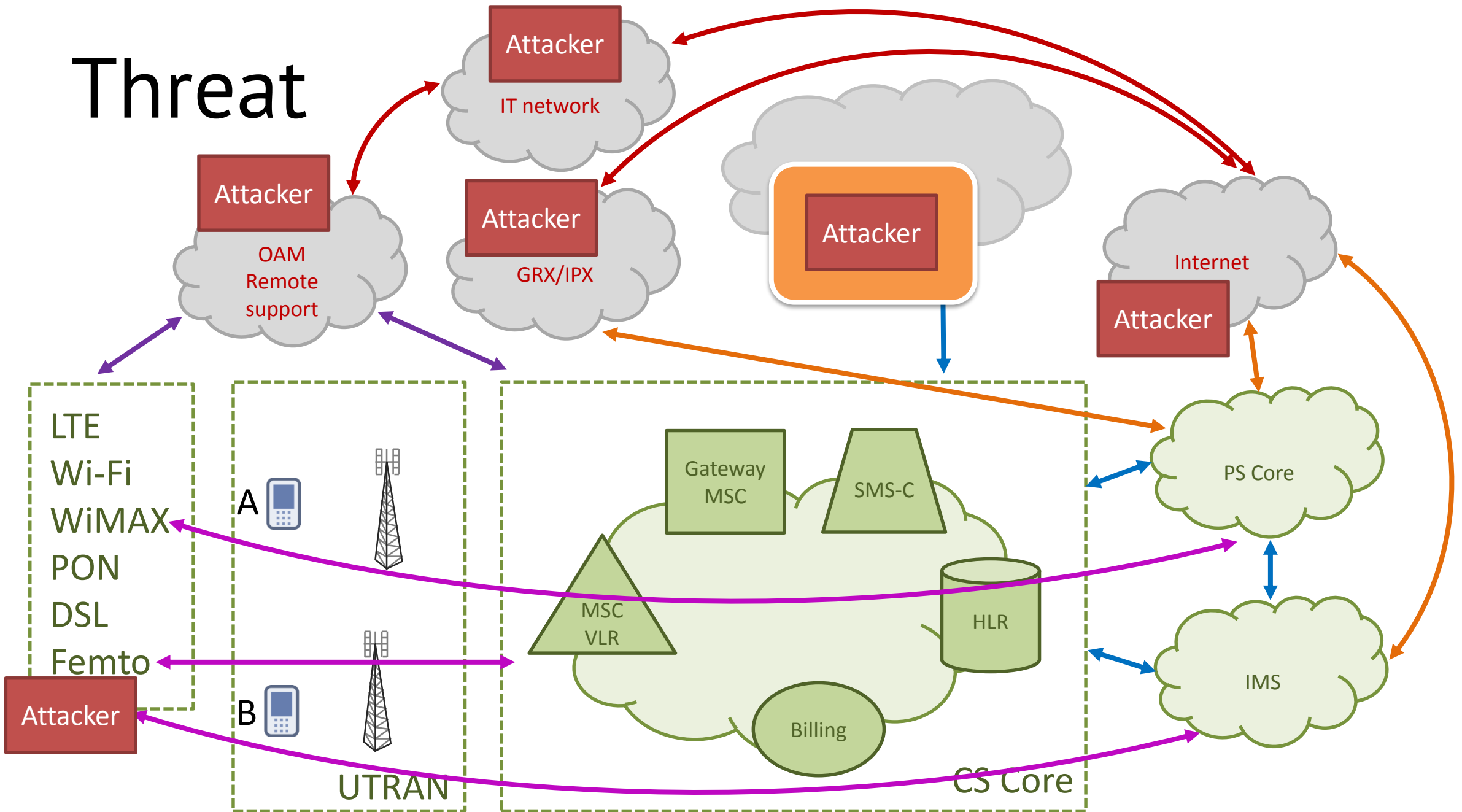
# Traffic



# Threats

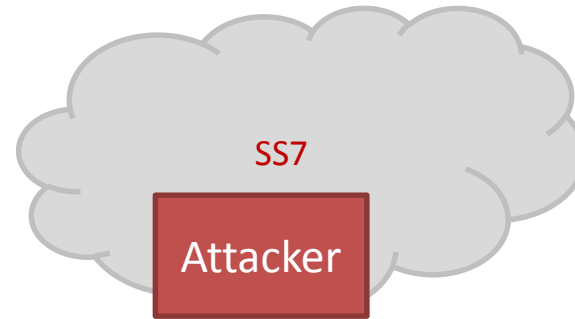


# Threat



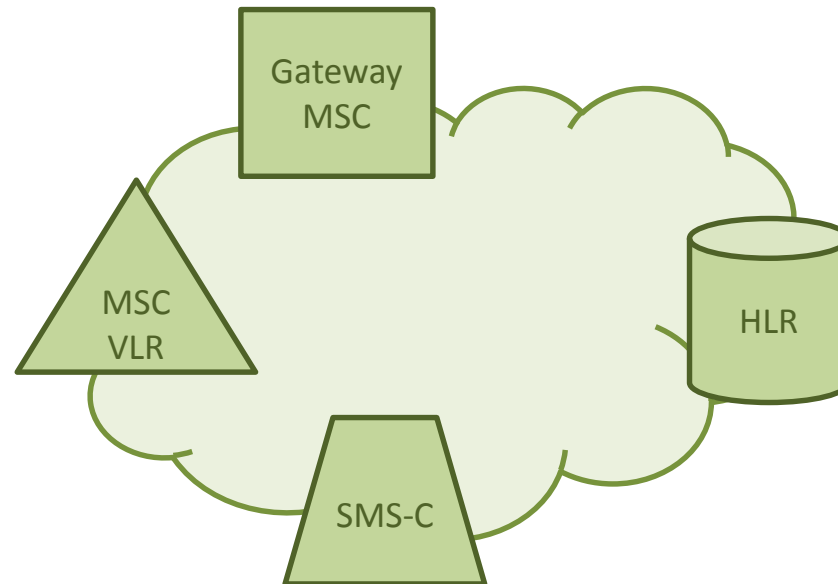
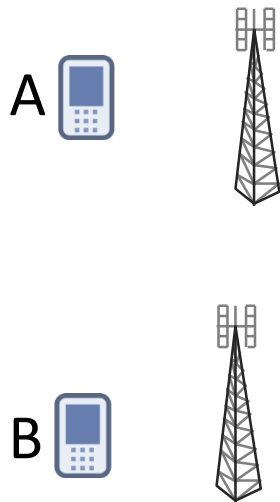
# SMS Interception

# Collect info



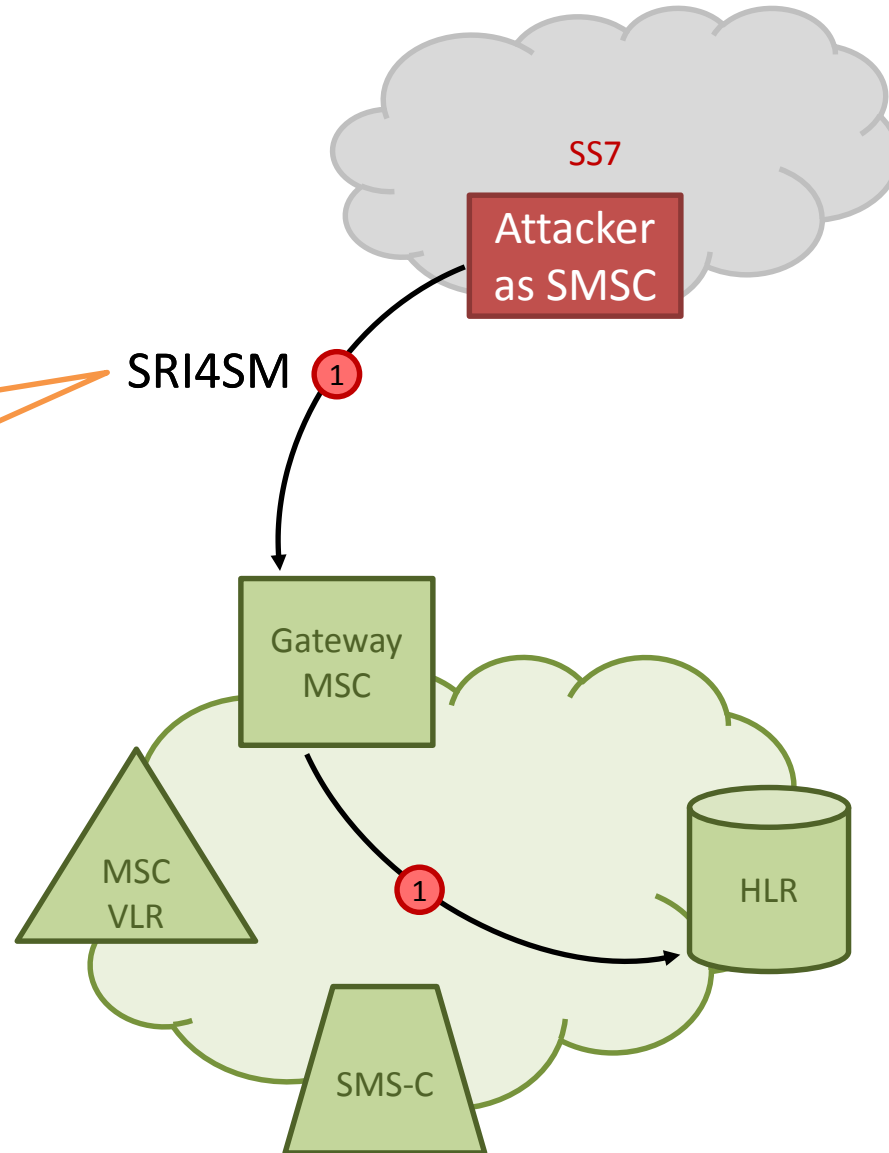
We know

**B-Number** 0 123 45678**02**



# Collect info

**sendRoutingInfoForSM**  
I am **SMSC**.  
**My GT** 1 321 4567801.  
Where is  
**Subscriber-B MSISDN** 0 123 4567802?



We know

**B-Number** 0 123 4567802

# Collect info

We know

**B-Number** 0 123 4567802

Protocol Length Info

GSM MAP 194 invoke sendRoutingInfoForSM

GSM MAP 206 returnResultLast sendRoutingInfoForSM

Called Party address (11 bytes)

Calling Party address (11 bytes)

Address Indicator

SubSystem Number: HLR (Home Location Register) (6)

[Linked to TCAP]

Global Title 0x4 (9 bytes)

Translation Type: 0x00

0001 .... = Numbering Plan: ISDN/telephony (0x01)

.... 0001 = Encoding Scheme: BCD, odd number of digits (0x01)

...000 0100 = Nature of Address Indicator: International number (0x04)

Calling Party Digits: HLR 0 123 4567800

Transaction Capabilities Application Part

GSM Mobile Application

Component: returnResultLast (2)

returnResultLast

invokeID: 1

resultretres

opCode: localValue (0)

imsi: Subscriber-B IMSI 15 digits

TBCD digits:

locationInfoWithLMSI

networkNode-Number: MSC/VLR 0 123 4567803

1... .... = Extension: No Extension

.001 .... = Nature of number: International Number (0x01)

0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x01)

Address digits:

## sendRoutingInfoForSM

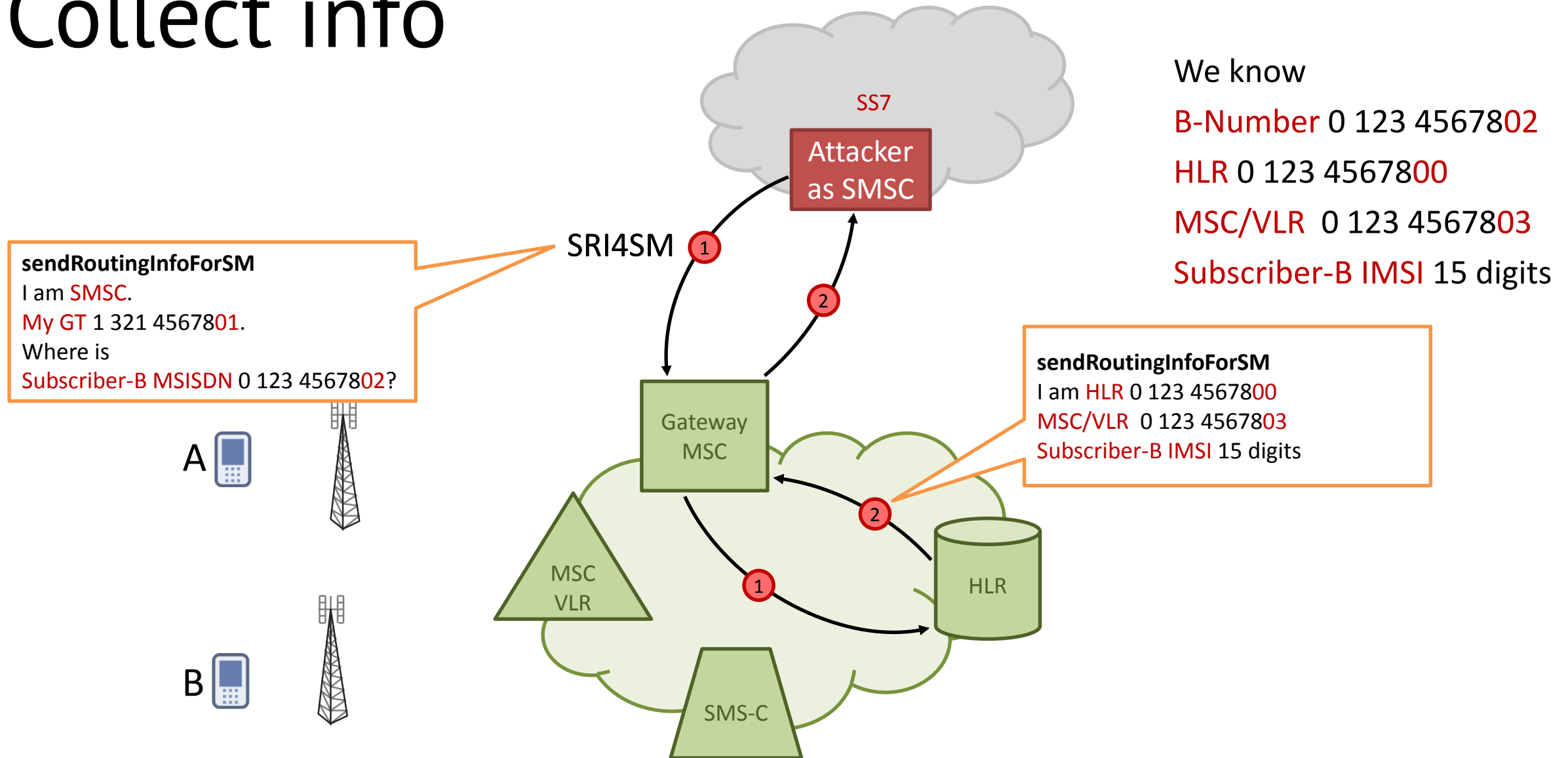
I am HLR 0 123 4567800

MSC/VLR 0 123 4567803

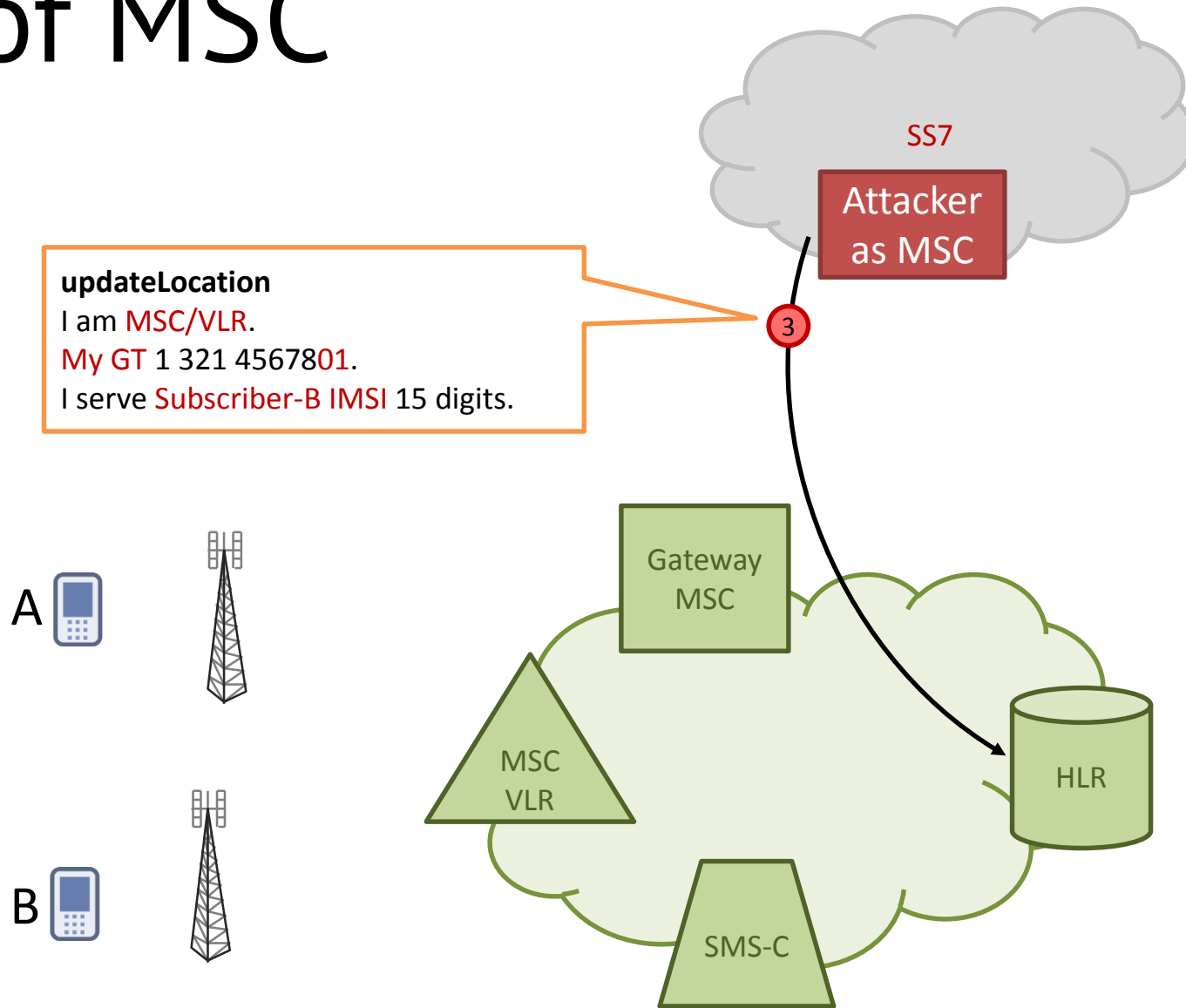
Subscriber-B IMSI 15 digits



# Collect info



# Spoof MSC



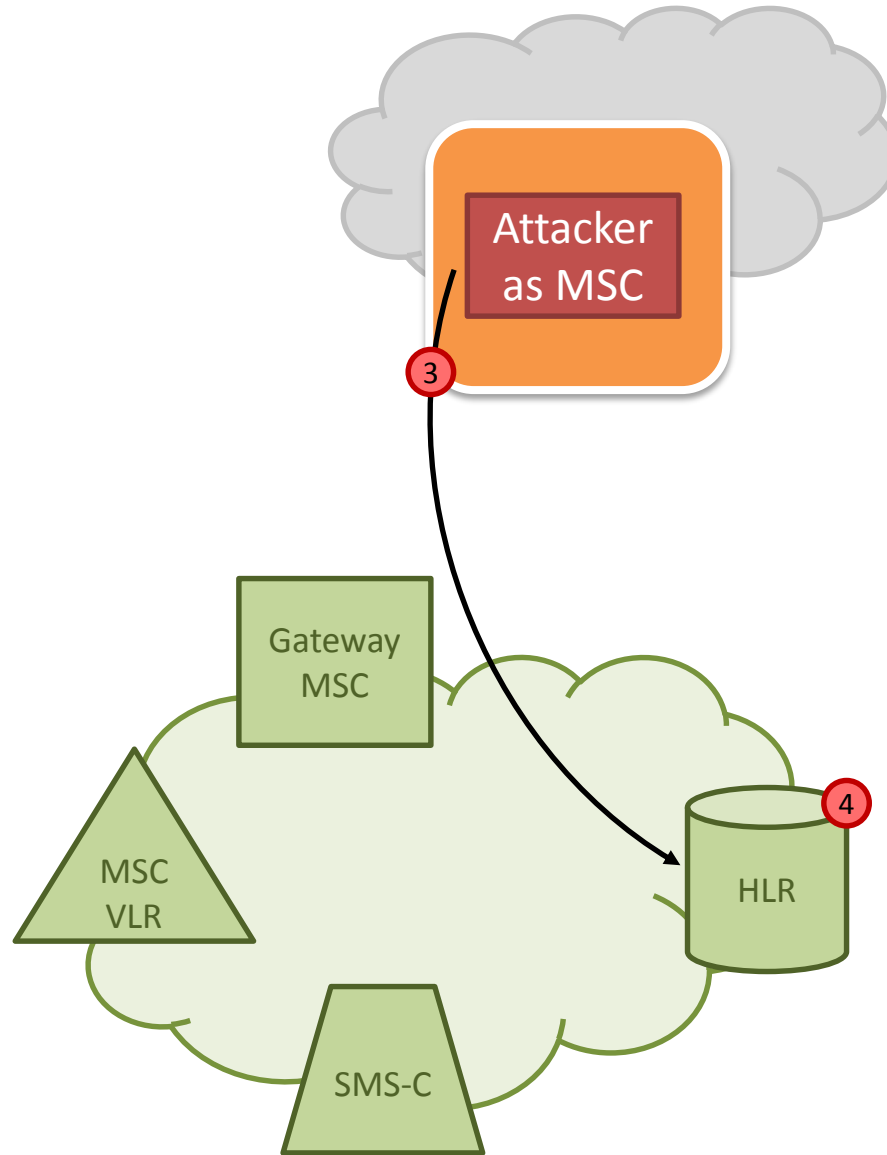
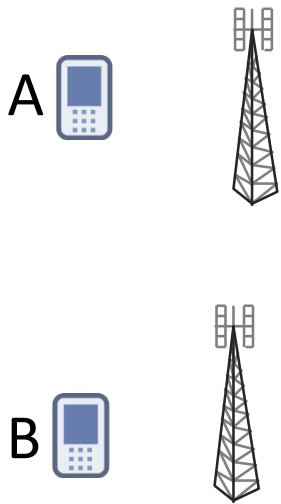
We know

**HLR 0 123 4567800**

**Subscriber-B IMSI 15 digits**

# Spoof MSC

Attacker serves  
Subscriber-B



We know

HLR 0 123 4567800

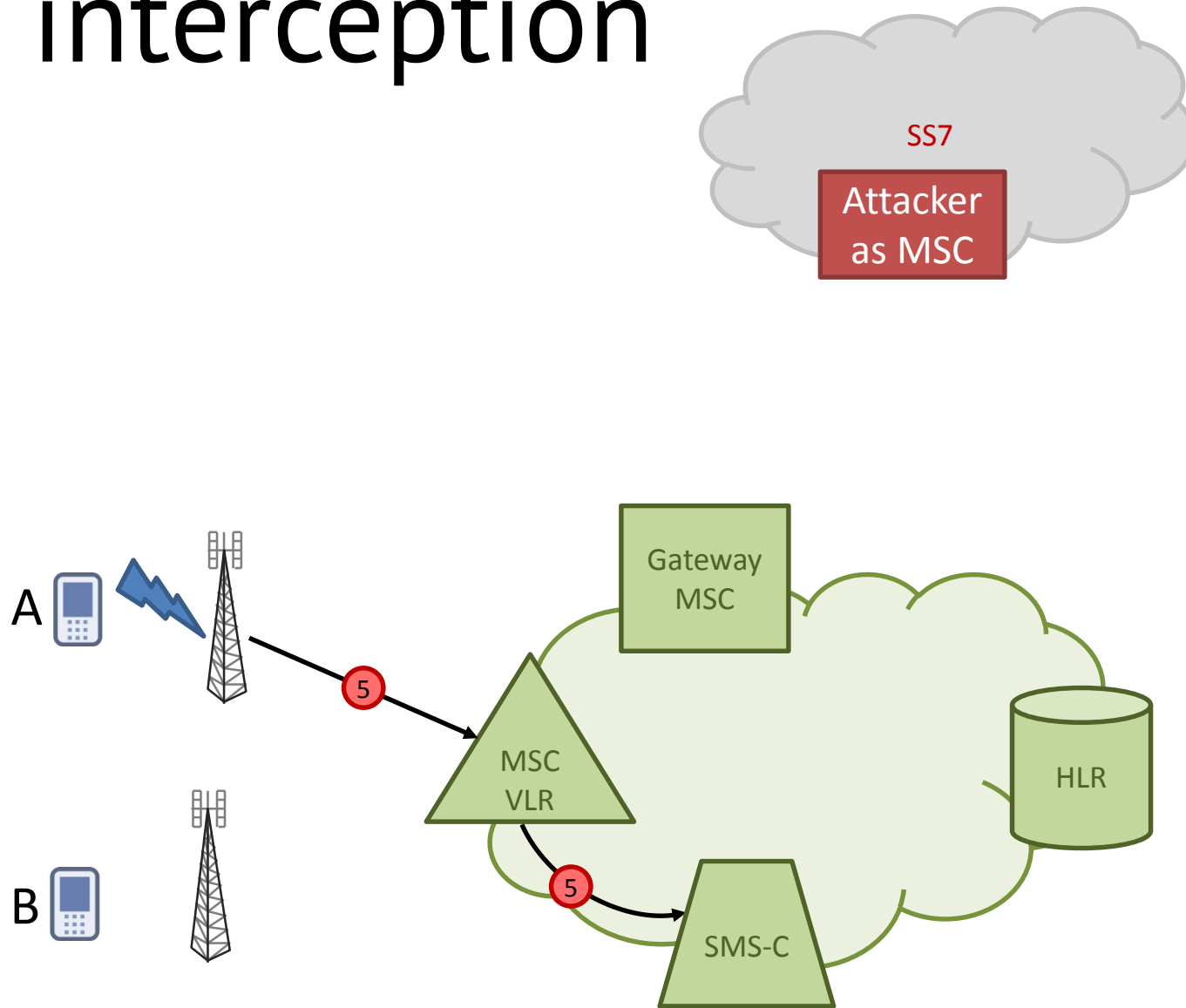
Subscriber-B IMSI 15 digits

HLR stores

Subscriber-B IMSI 15 digits

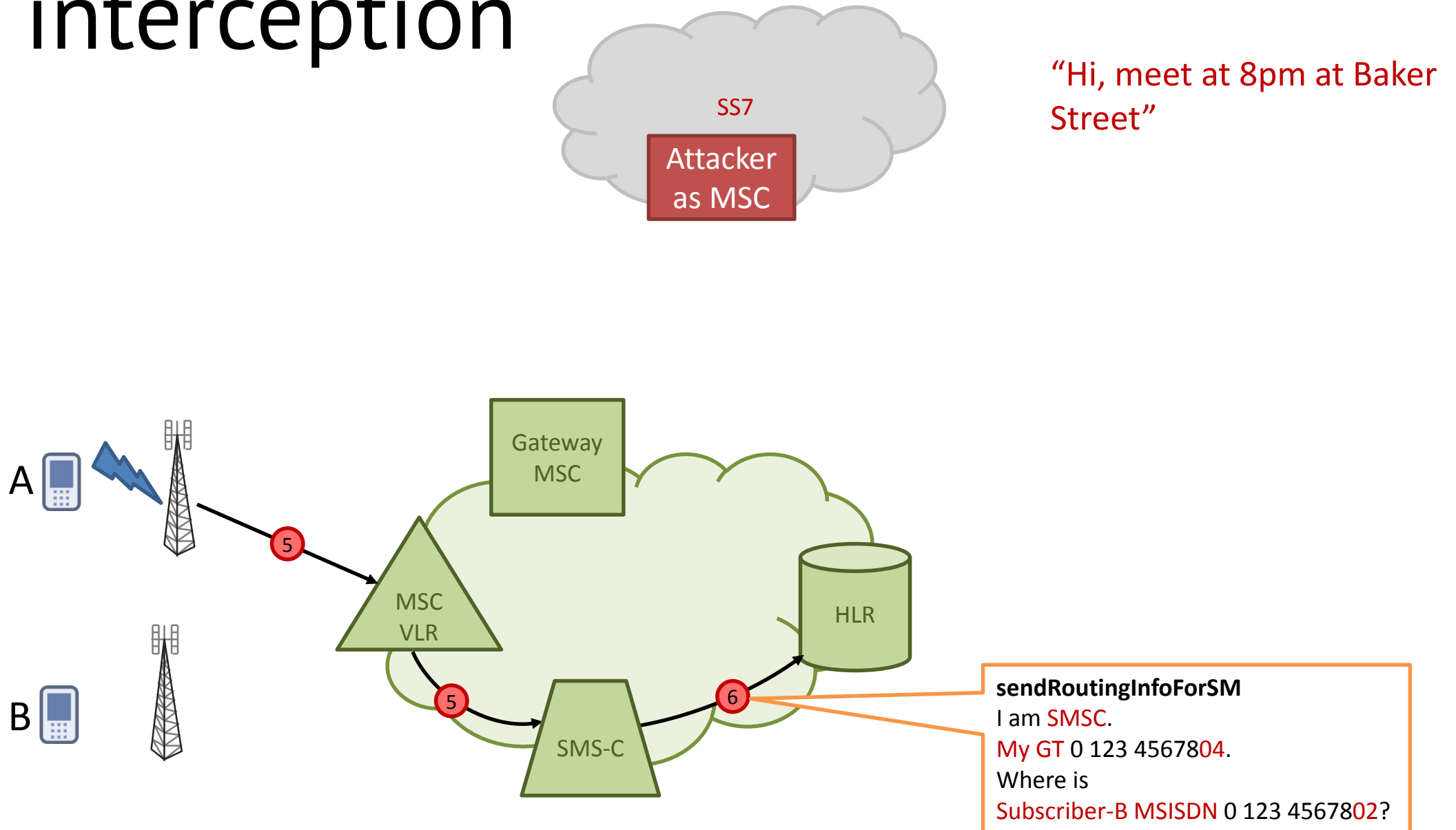
MSC/VLR 1 321 4567801

# SMS interception

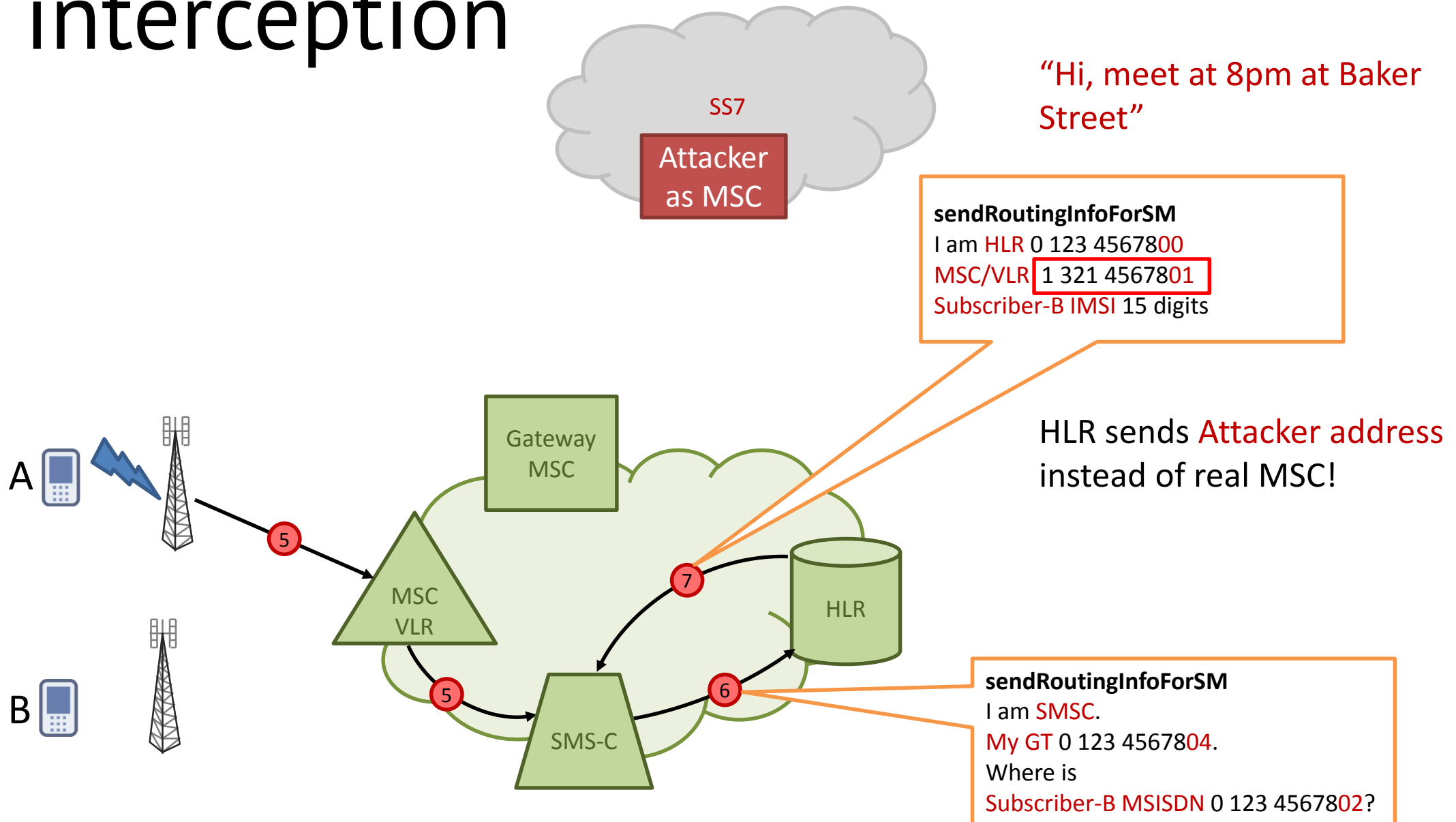


“Hi, meet at 8pm at Baker Street”

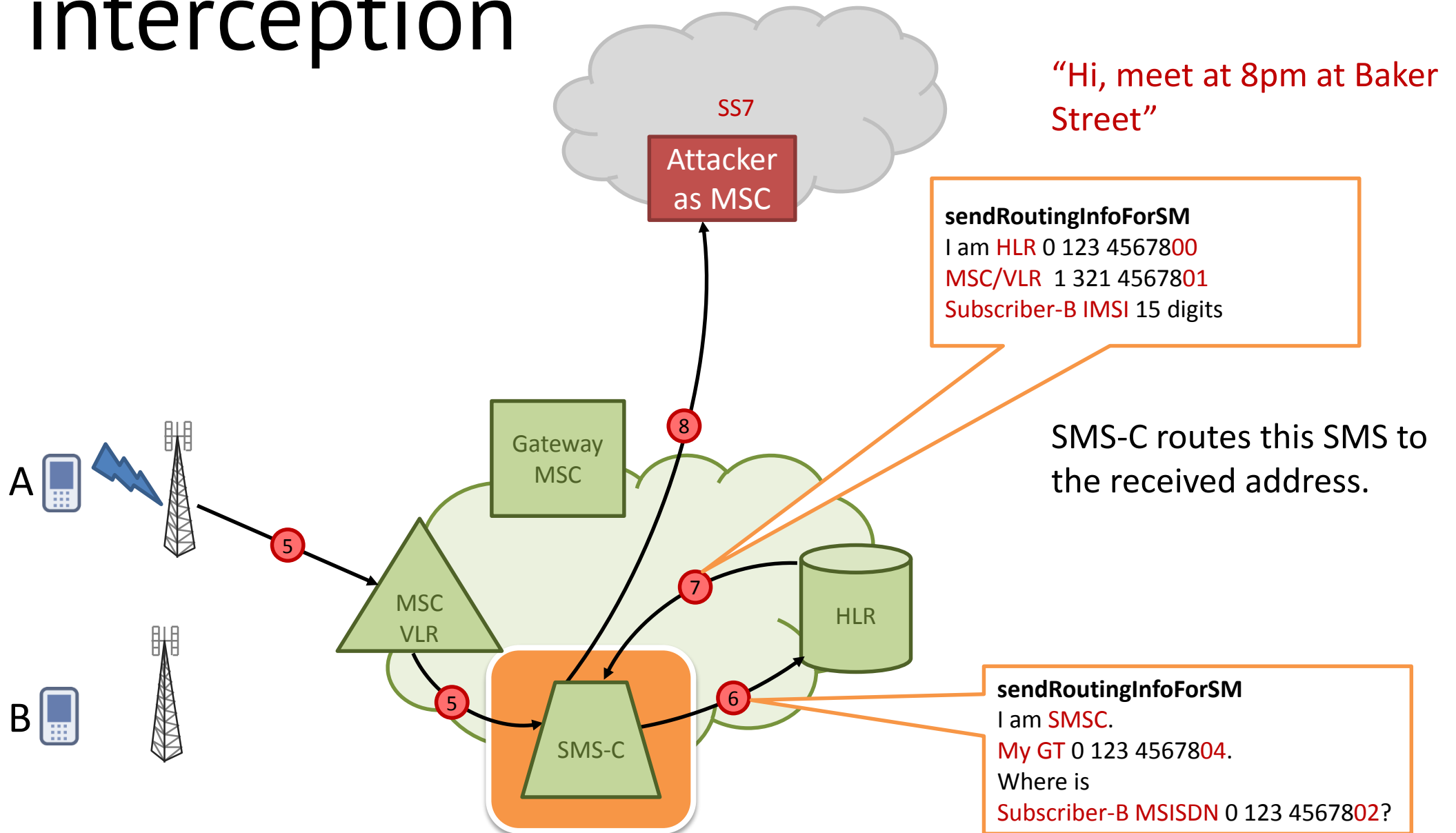
# SMS interception



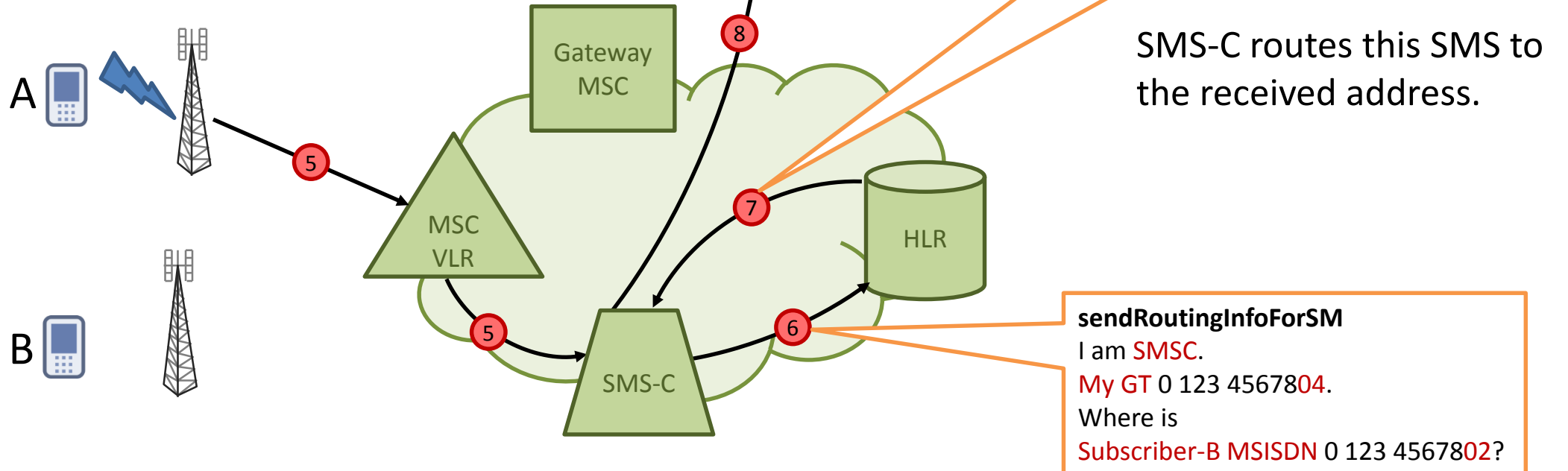
# SMS interception



# SMS interception



# SMS interception





# SMS interception



1. SMS chats
2. One time passwords
3. Notifications
4. Password recovery

# Money Transfer

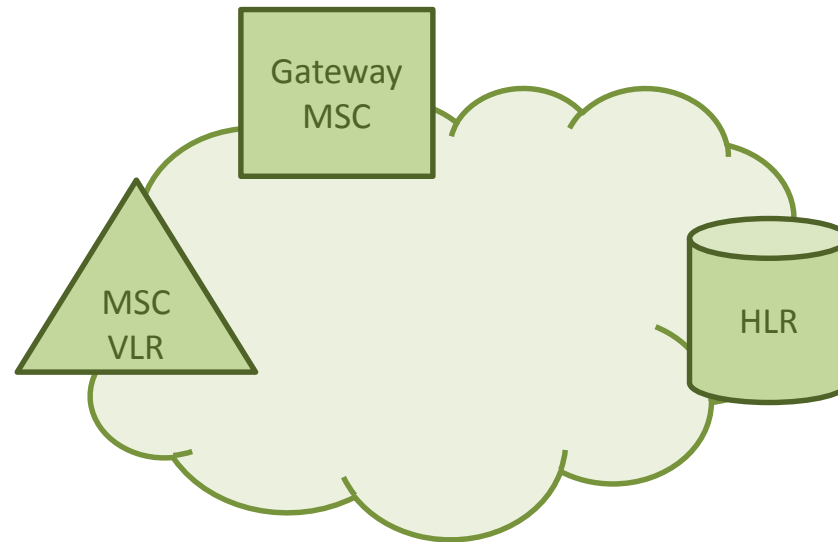
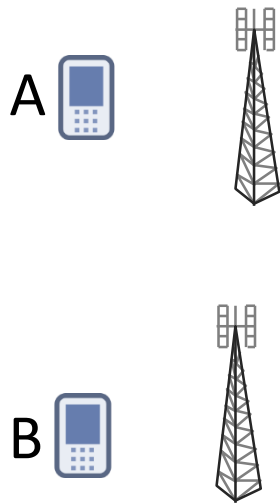
## Using USSD

# Collect info

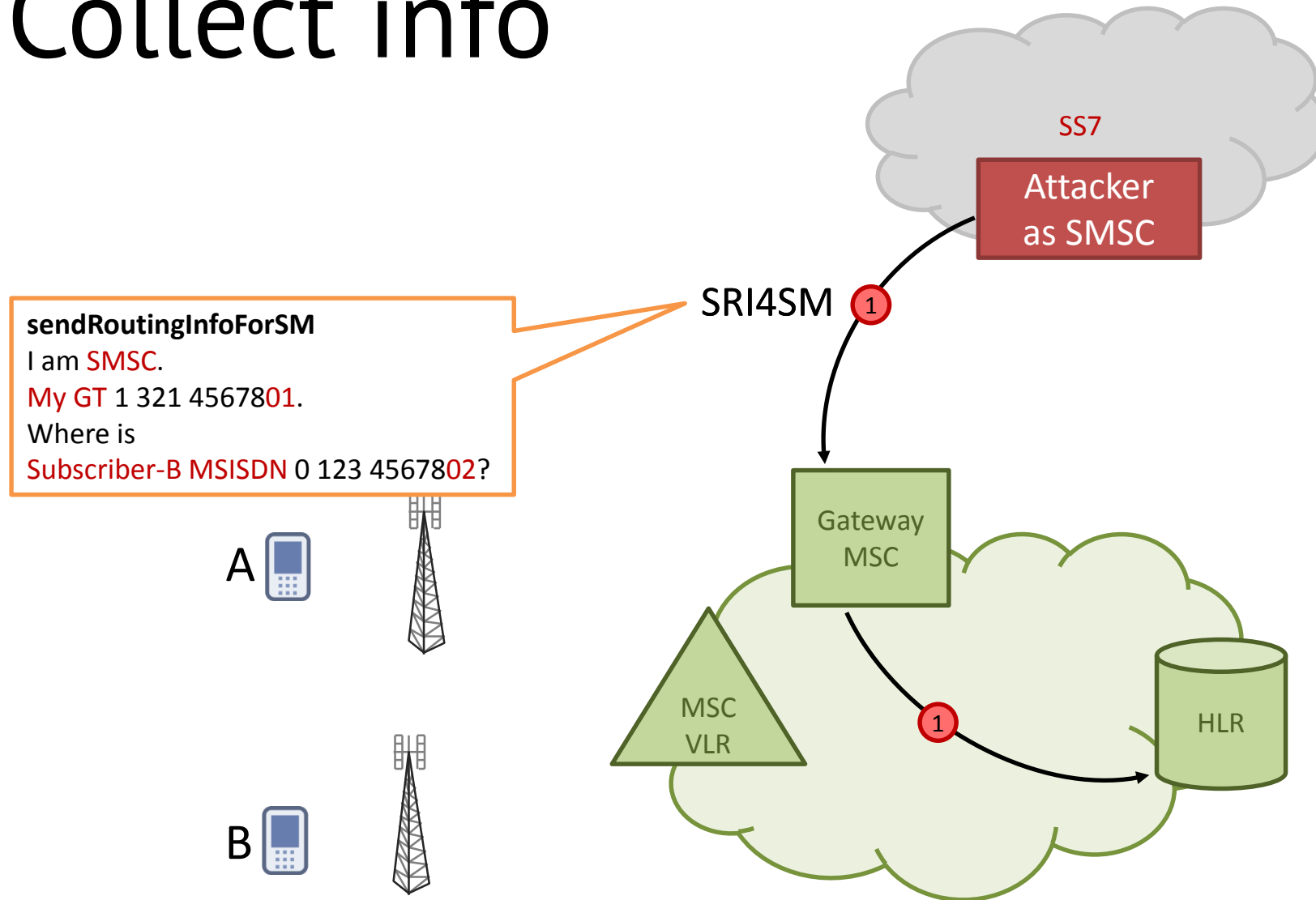


We know

**B-Number** 0 123 45678**02**



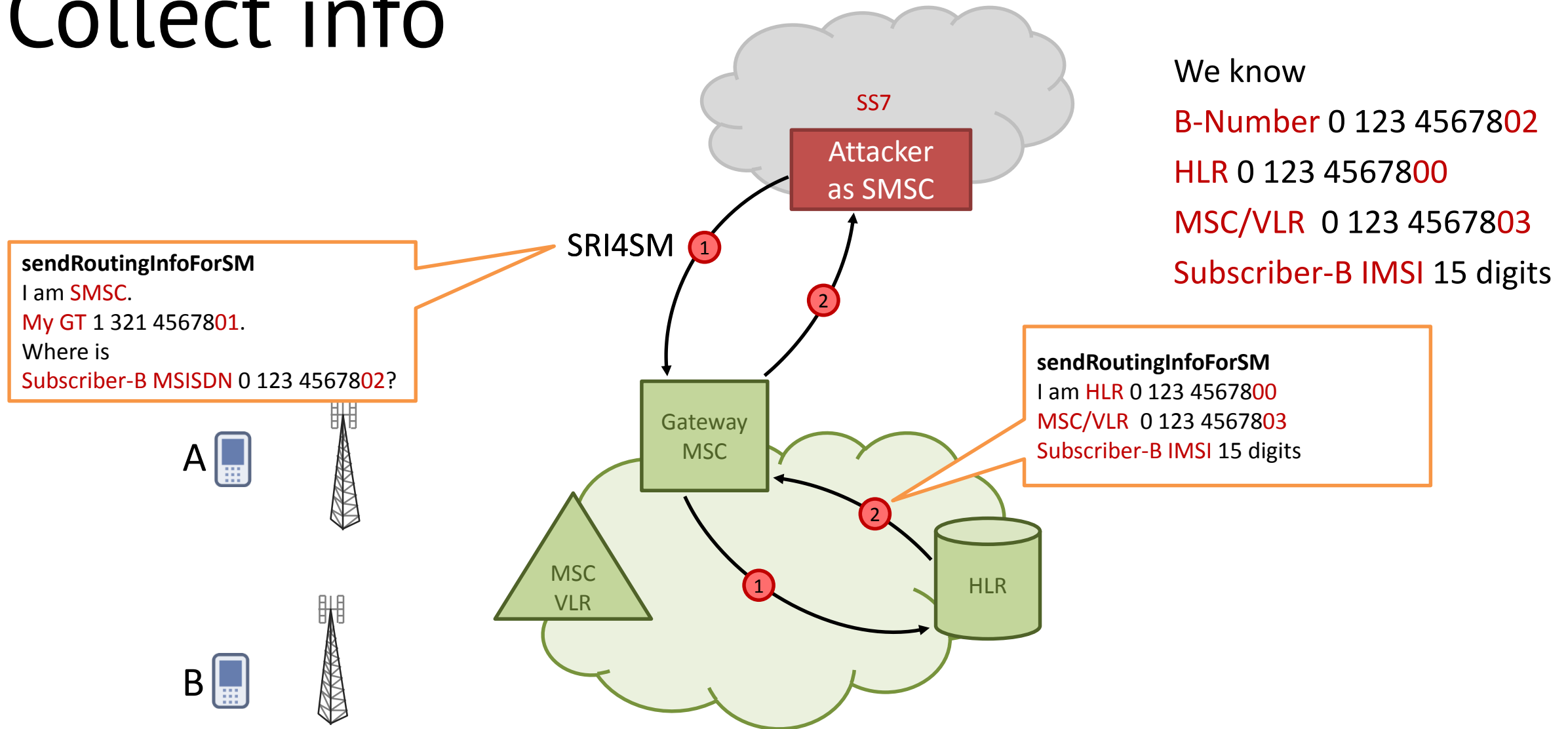
# Collect info



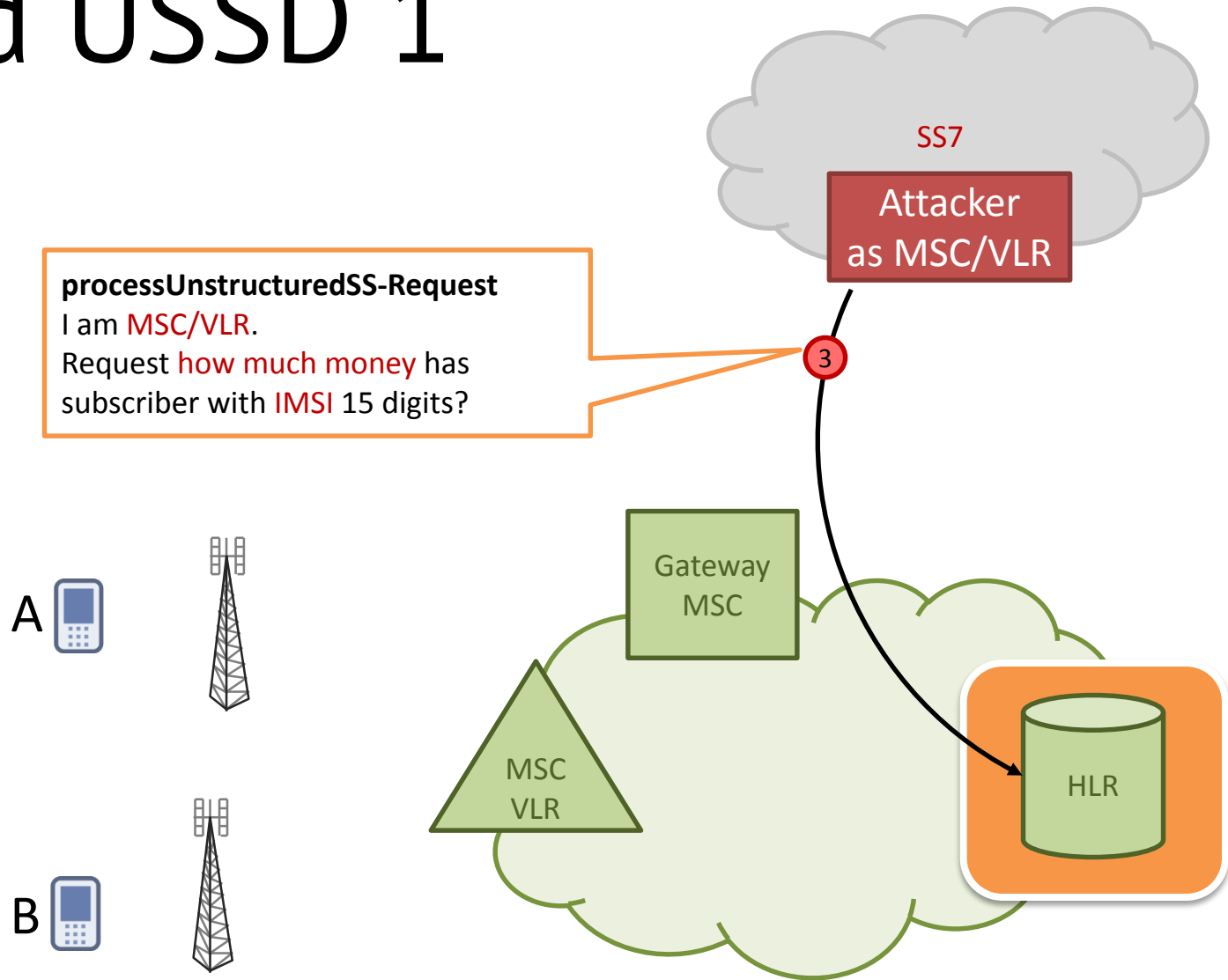
We know

**B-Number** 0 123 4567802

# Collect info



# Send USSD 1



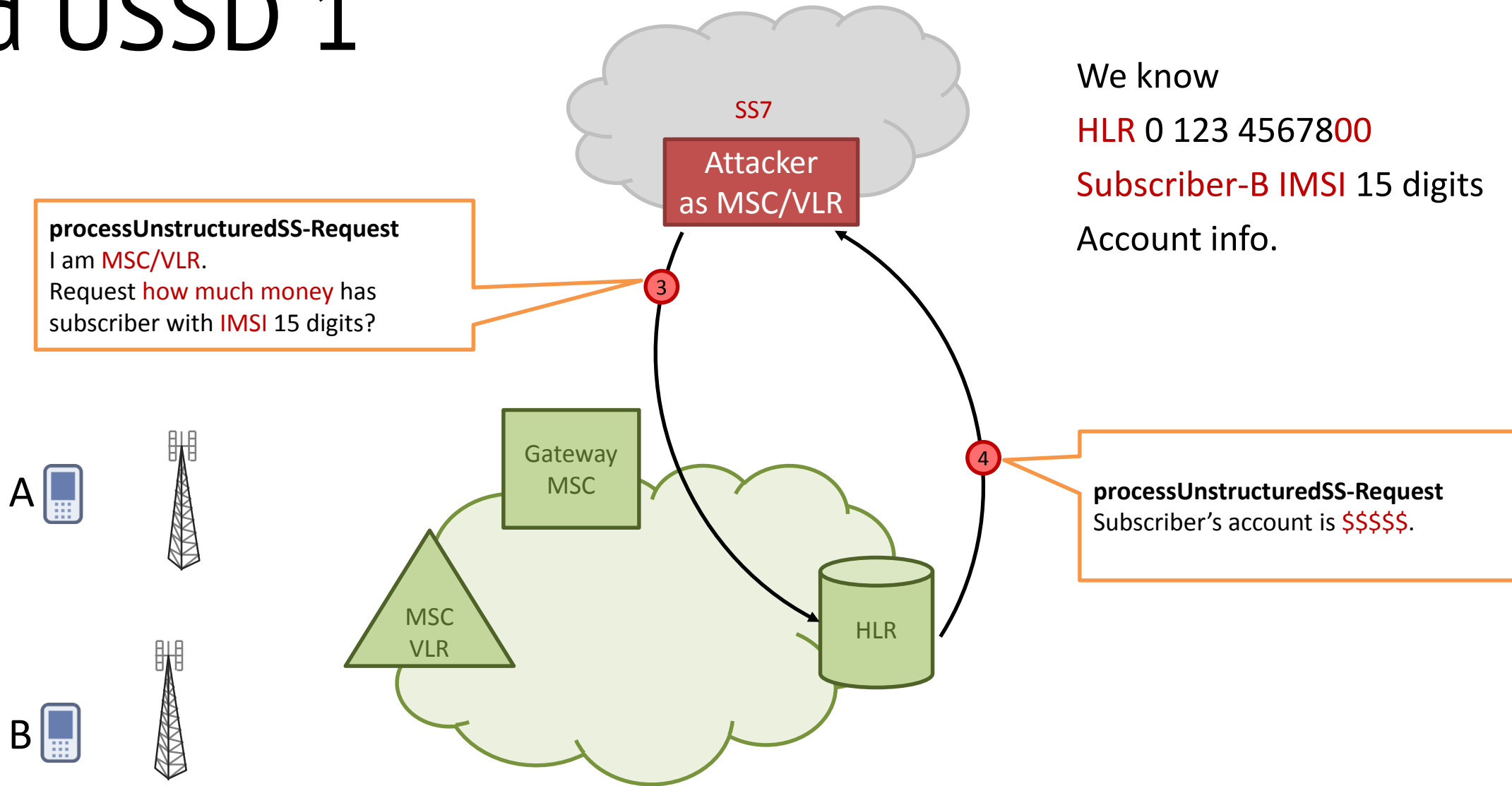
We know

**HLR 0 123 4567800**

**Subscriber-B IMSI 15 digits**

**\*100#**

# Send USSD 1



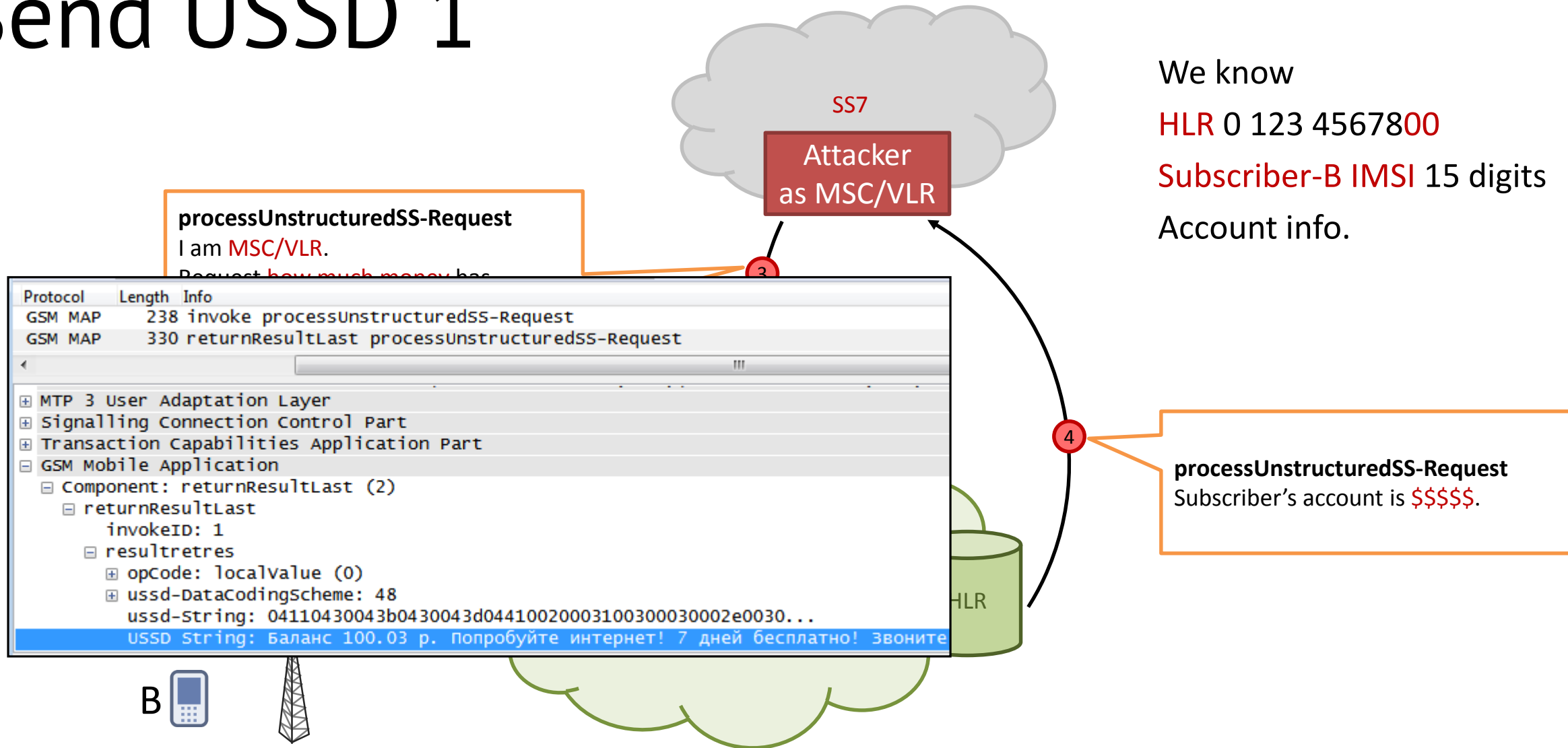
# Send USSD 1

We know

HLR 0 123 4567800

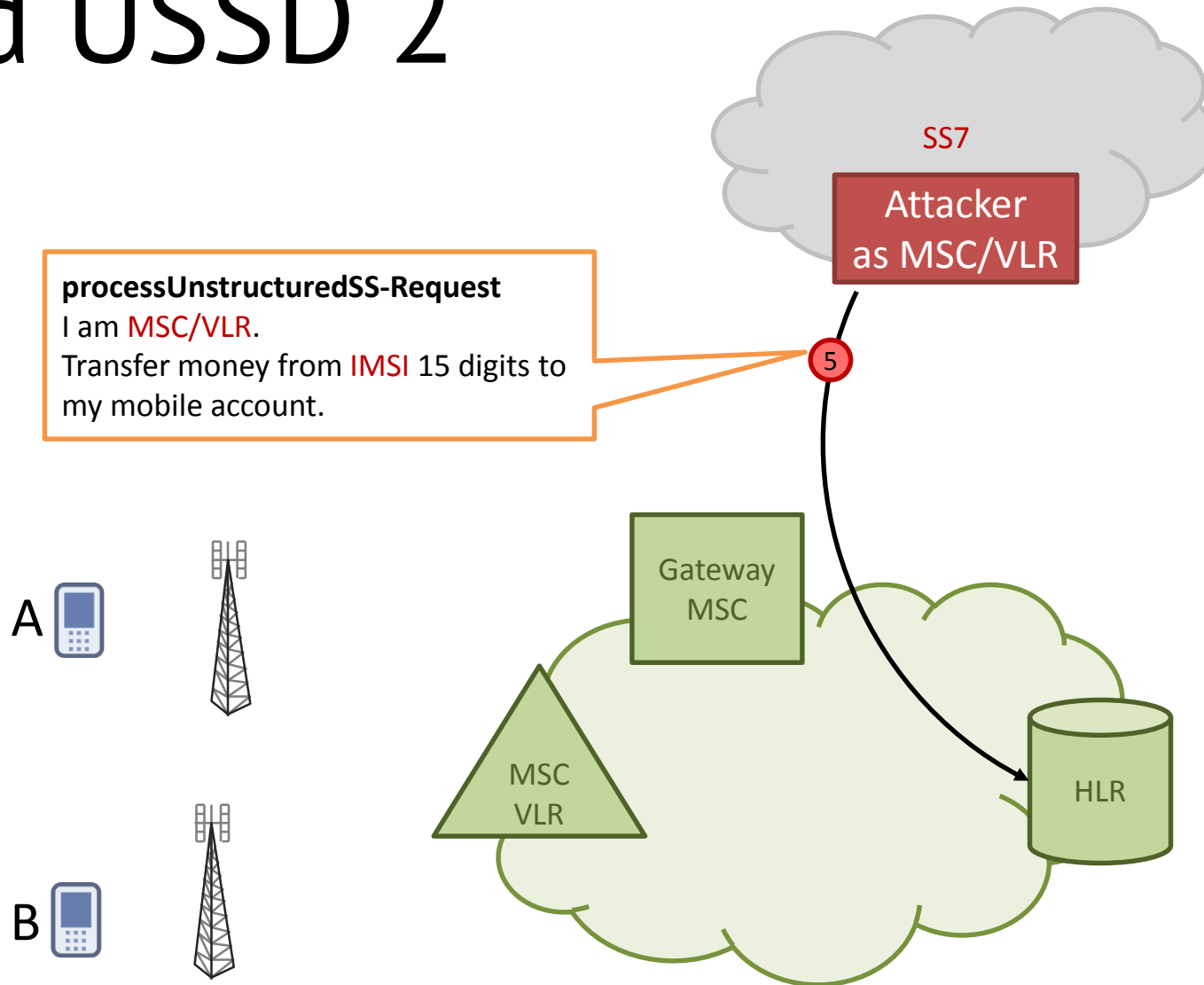
Subscriber-B IMSI 15 digits

Account info.





# Send USSD 2



We know

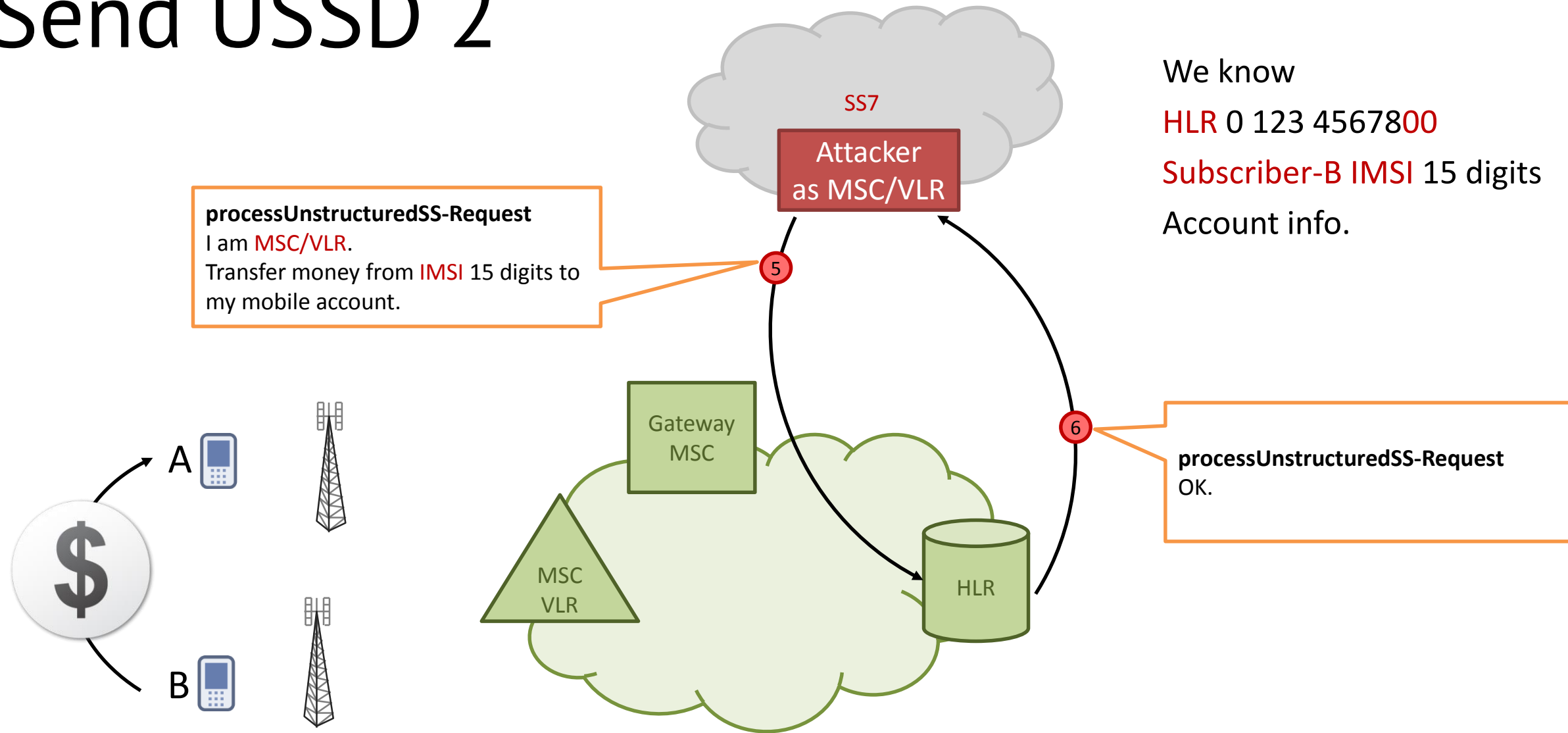
HLR 0 123 4567800

Subscriber-B IMSI 15 digits

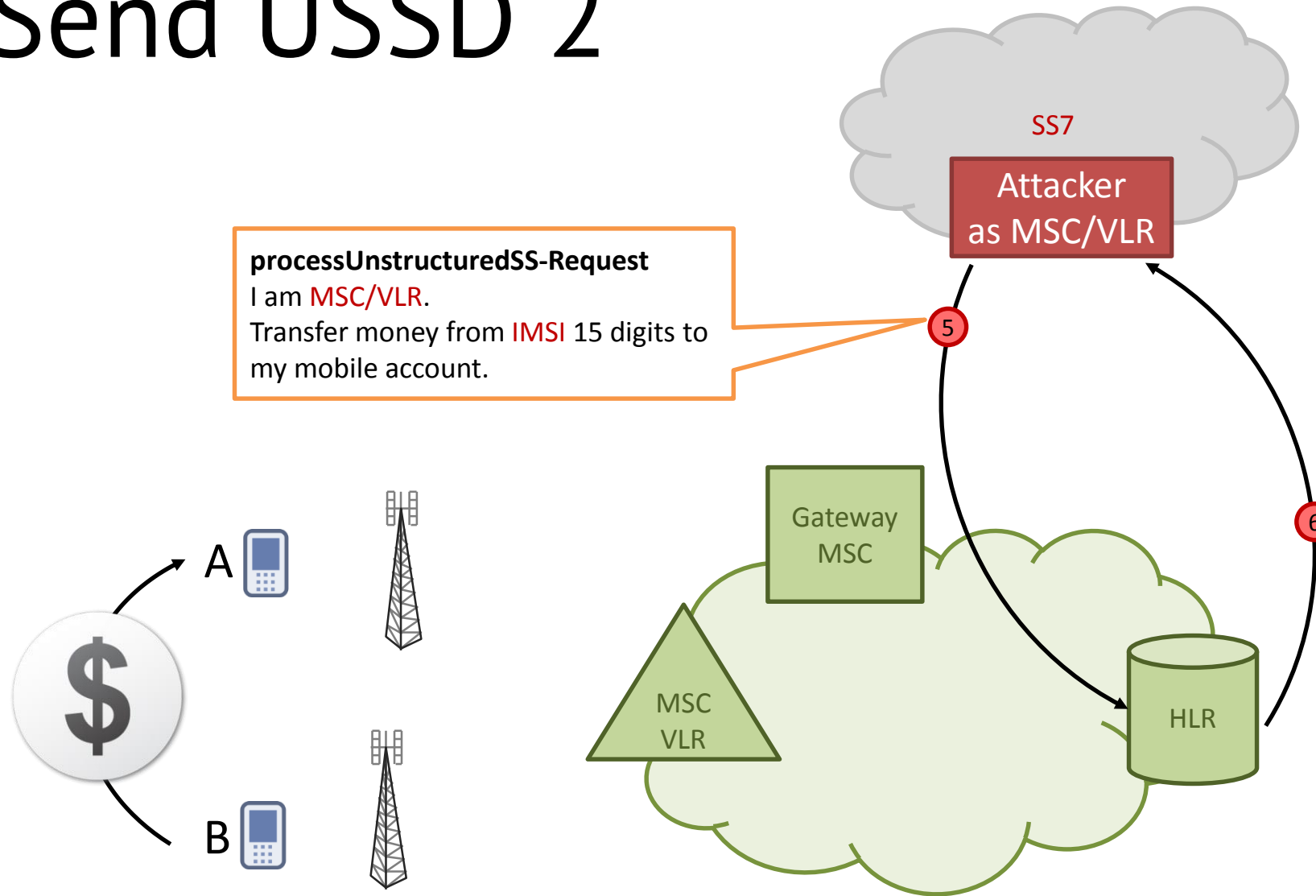
Account info.

**\*123\*01238765400\*100#**

# Send USSD 2



# Send USSD 2



**Real account info.**

Subscriber B does not get SMS notification if Attacker combines this attack and the previous one.

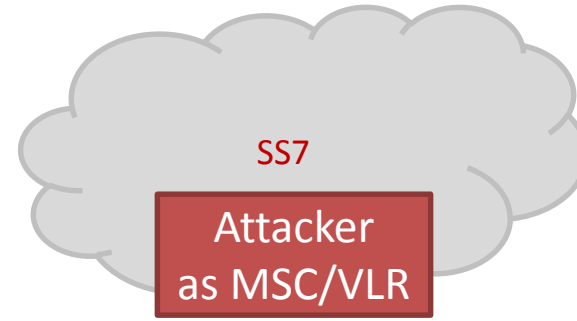
# Send USSD 2



**processUnstructuredSS-Request**

I am **MSC/VLR**.

Transfer money from **IMSI** 15 digits to my mobile account.



5

6



**Real account info.**

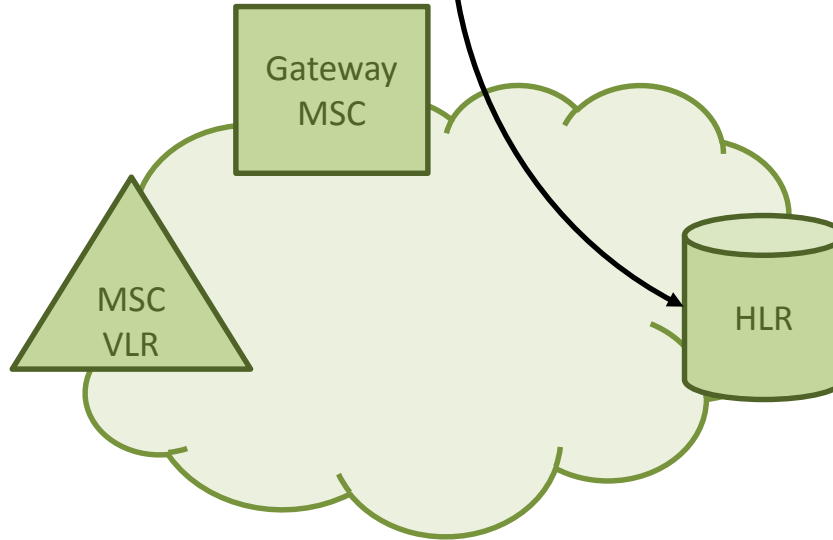
**processUnstructuredSS-Request**  
OK.



A



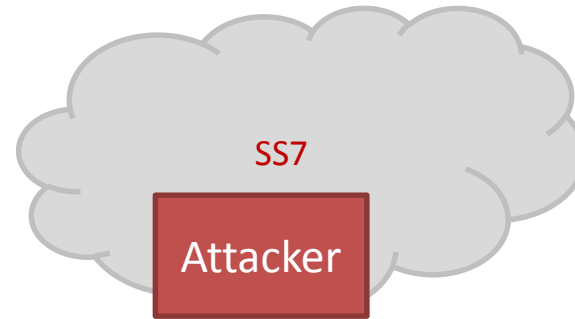
B



Subscriber B does not get SMS notification if Attacker combines this attack and the previous one.

# Mobile Switching Center DoS

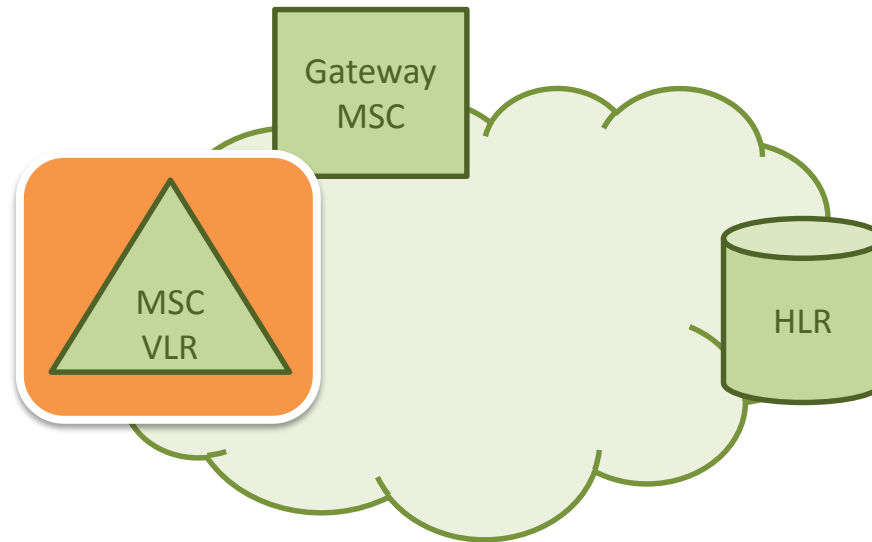
# Collect info



We know

**B-Number** 0 123 45678**02**

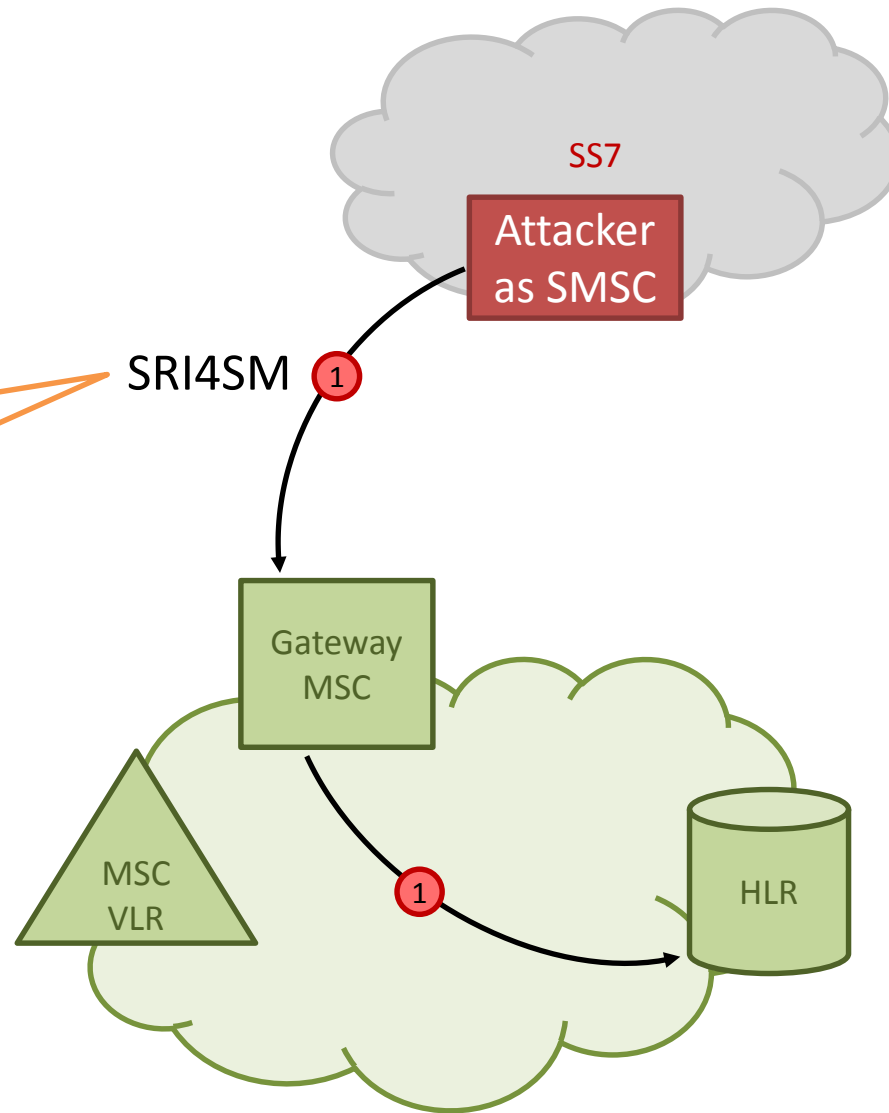
B



# Collect info

**sendRoutingInfoForSM**  
I am **SMSC**.  
**My GT** 1 321 45678**01**.  
Where is  
**Subscriber-B MSISDN** 0 123 45678**02**?

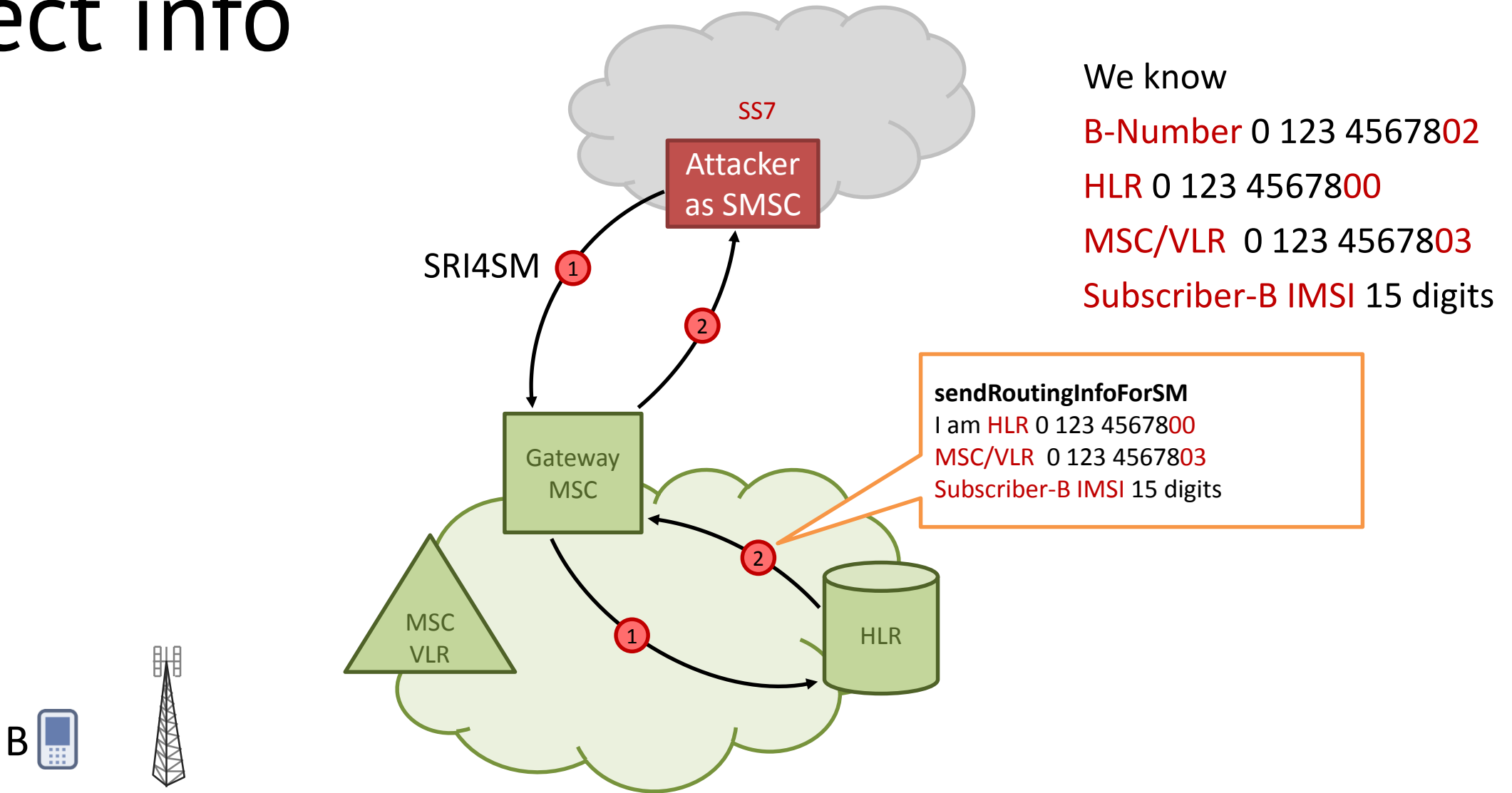
B 



We know

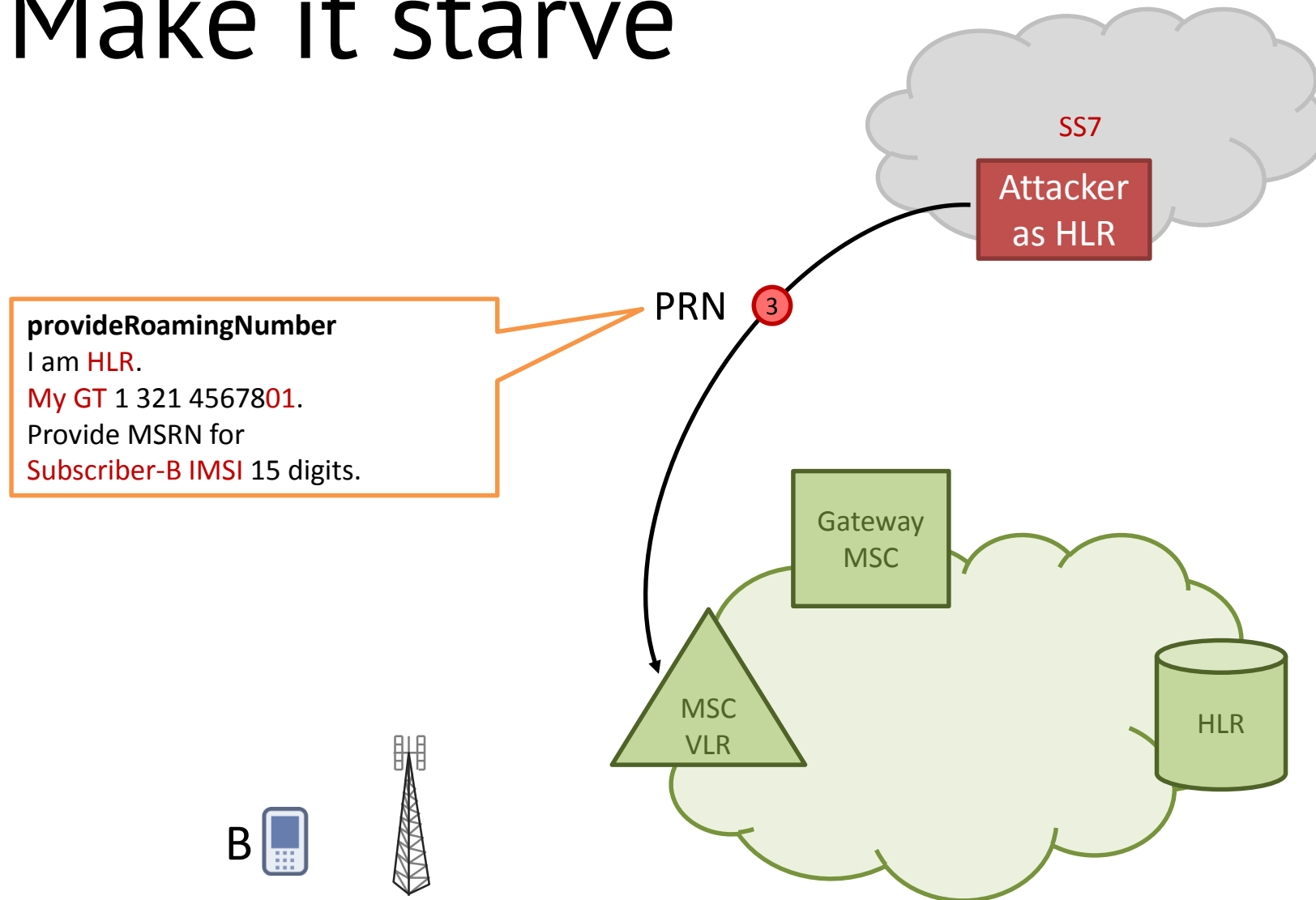
**B-Number** 0 123 45678**02**

# Collect info





# Make it starve

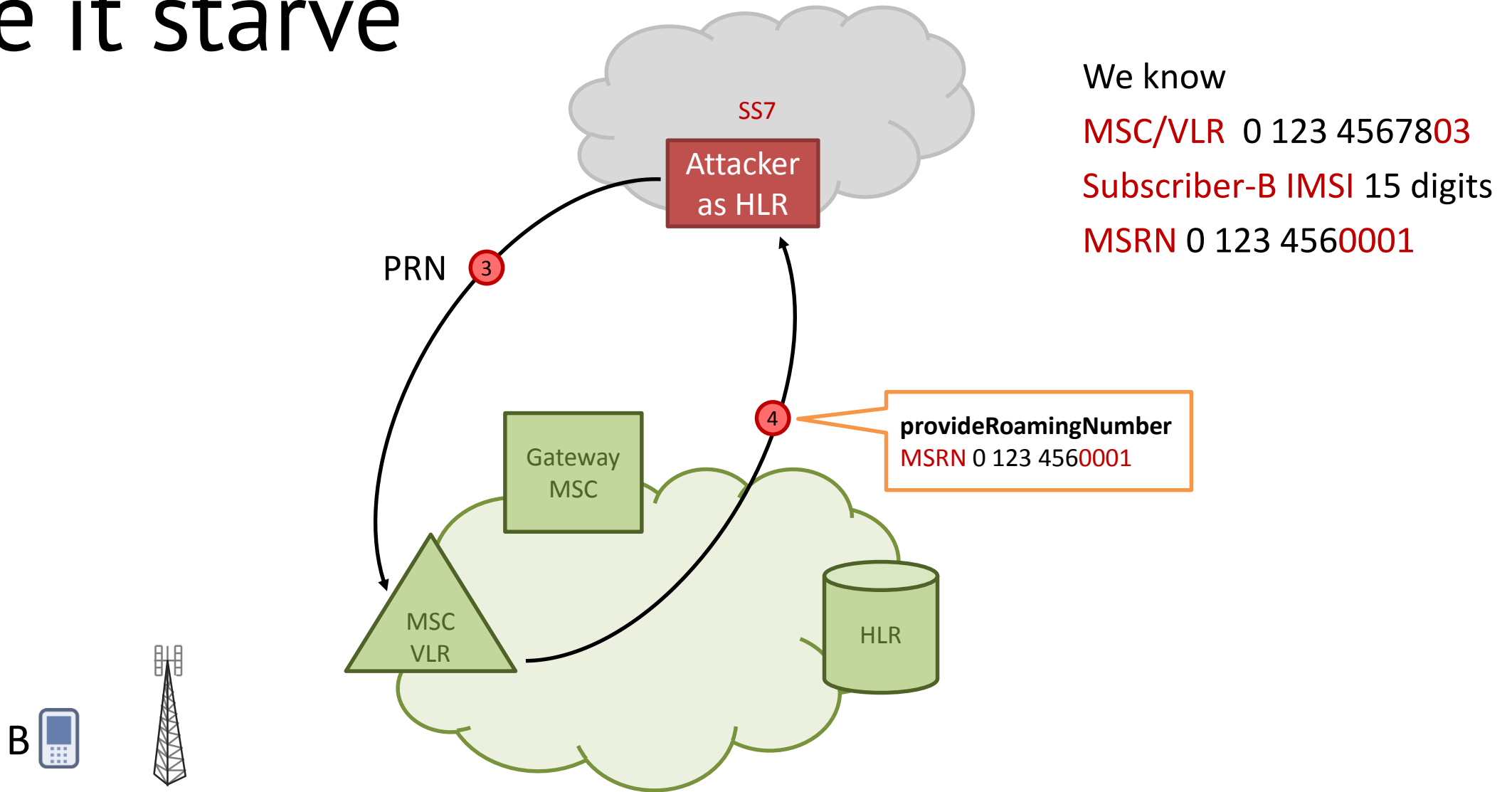


We know

**MSC/VLR** 0 123 45678**03**

**Subscriber-B IMSI** 15 digits

# Make it starve

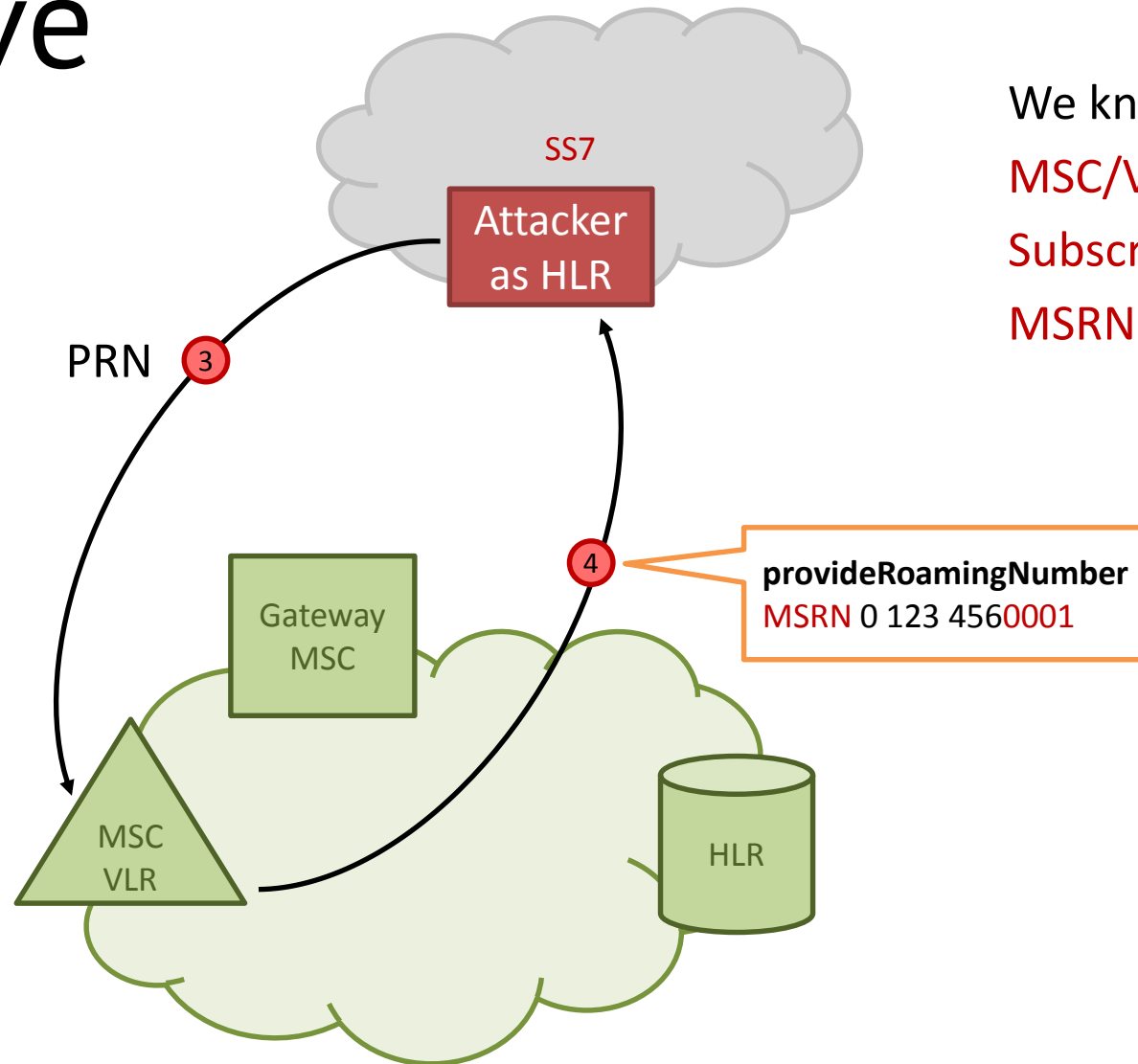


# Make it starve

Default timeouts for MSRN:

- Ericsson – 30 sec
- Huawei – 45 sec

B 



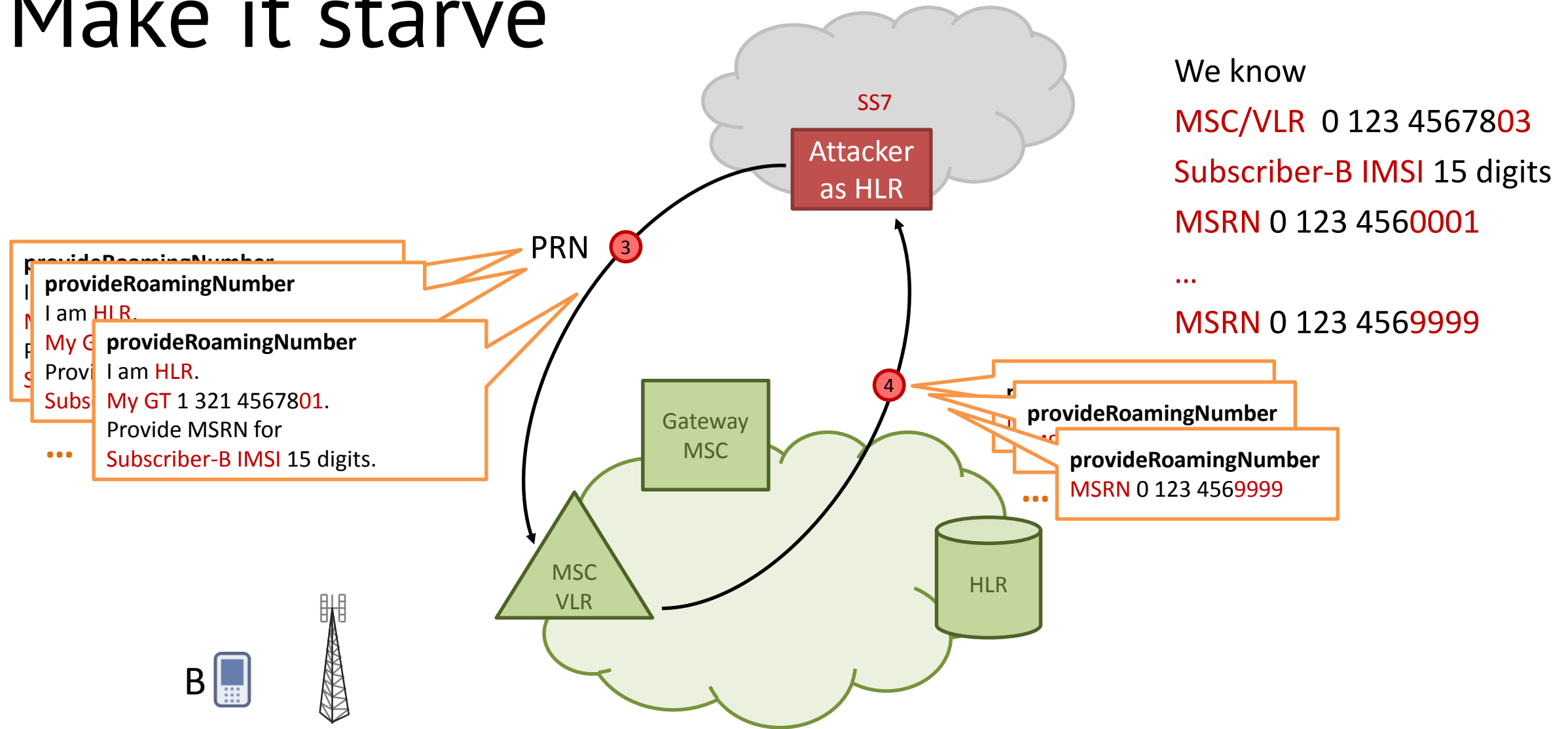
We know

MSC/VLR 0 123 4567803

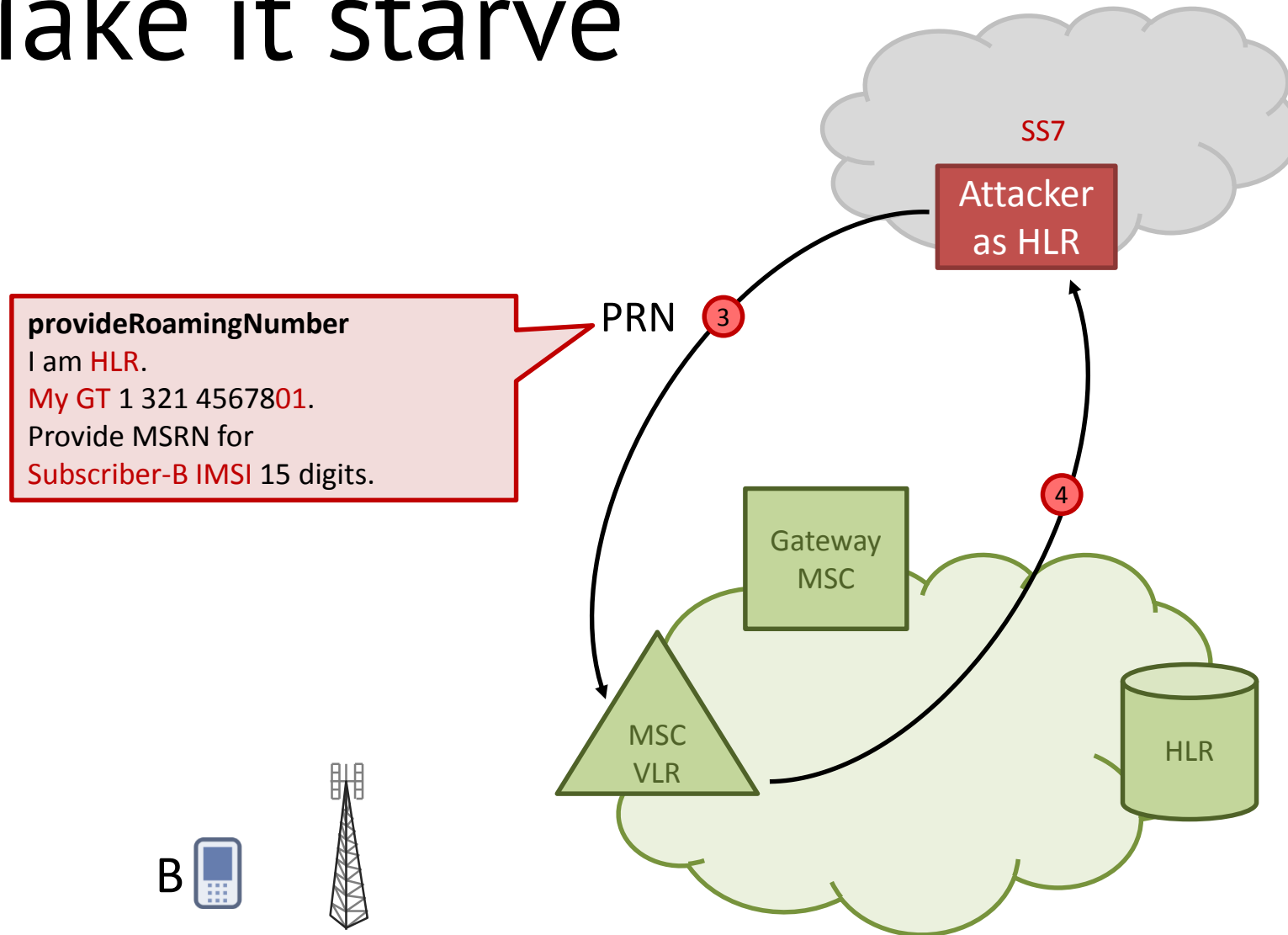
Subscriber-B IMSI 15 digits

MSRN 0 123 4560001

# Make it starve



# Make it starve



We know

**MSC/VLR 0 123 4567803**

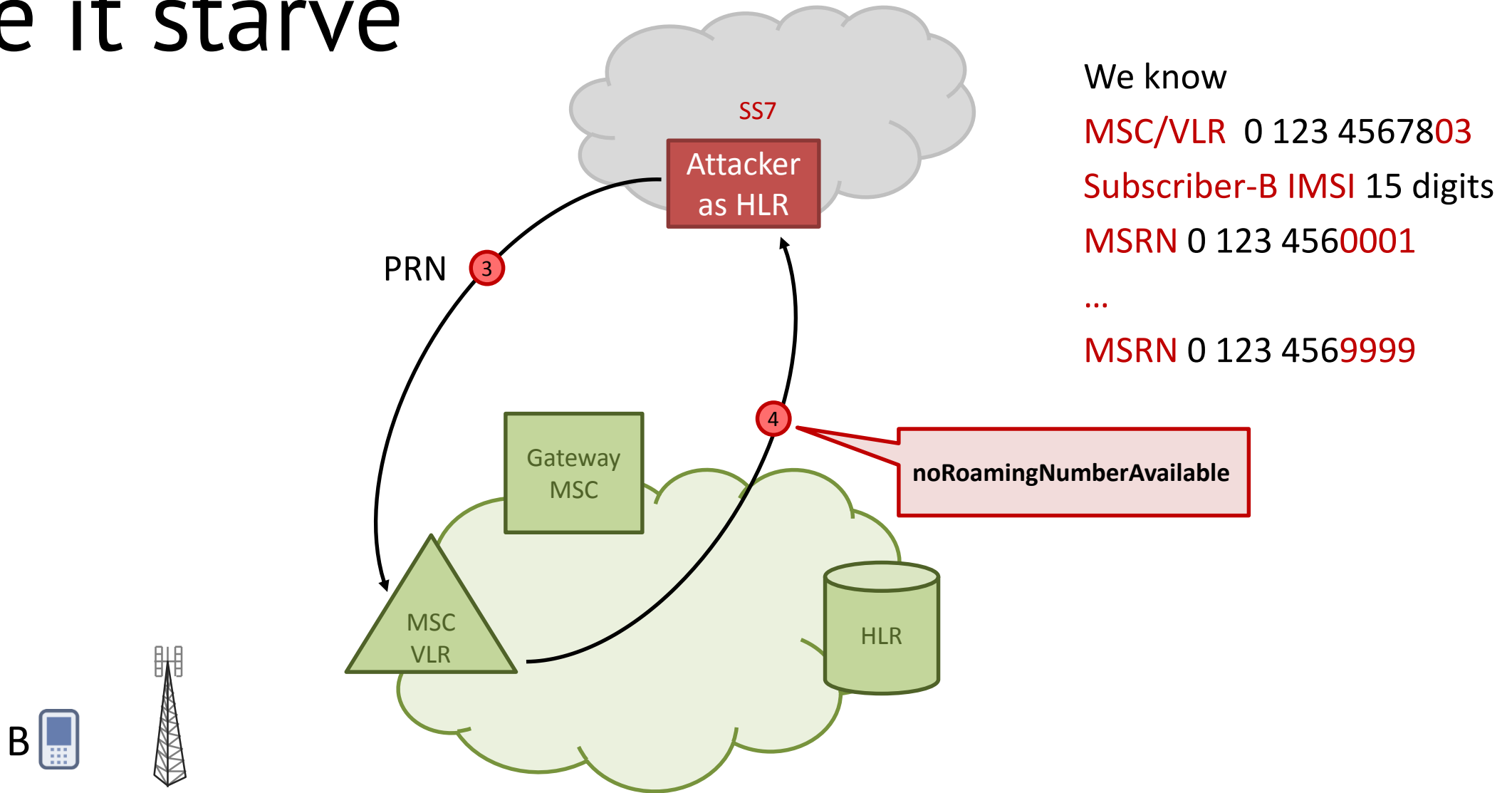
**Subscriber-B IMSI 15 digits**

**MSRN 0 123 4560001**

...

**MSRN 0 123 4569999**

# Make it starve



# Make it starve

The image shows a Wireshark packet capture of GSM MAP messages. The packet list on the left shows a sequence of 'invoke provideRoamingNumber' and 'returnResultLast provideRoamingNumber' messages. The selected packet (packet 4) is a 'returnError' message. The packet details pane on the right shows the 'returnError' structure with the following fields:

- Component: returnError (3)
- returnError
  - invokeID: 1
  - errorCode: localValue (0)
    - localValue: noRoamingNumberAvailable (39)

We know

MSC/VLR 0 123 4567803

Subscriber-B IMSI 15 digits

MSRN 0 123 4560001

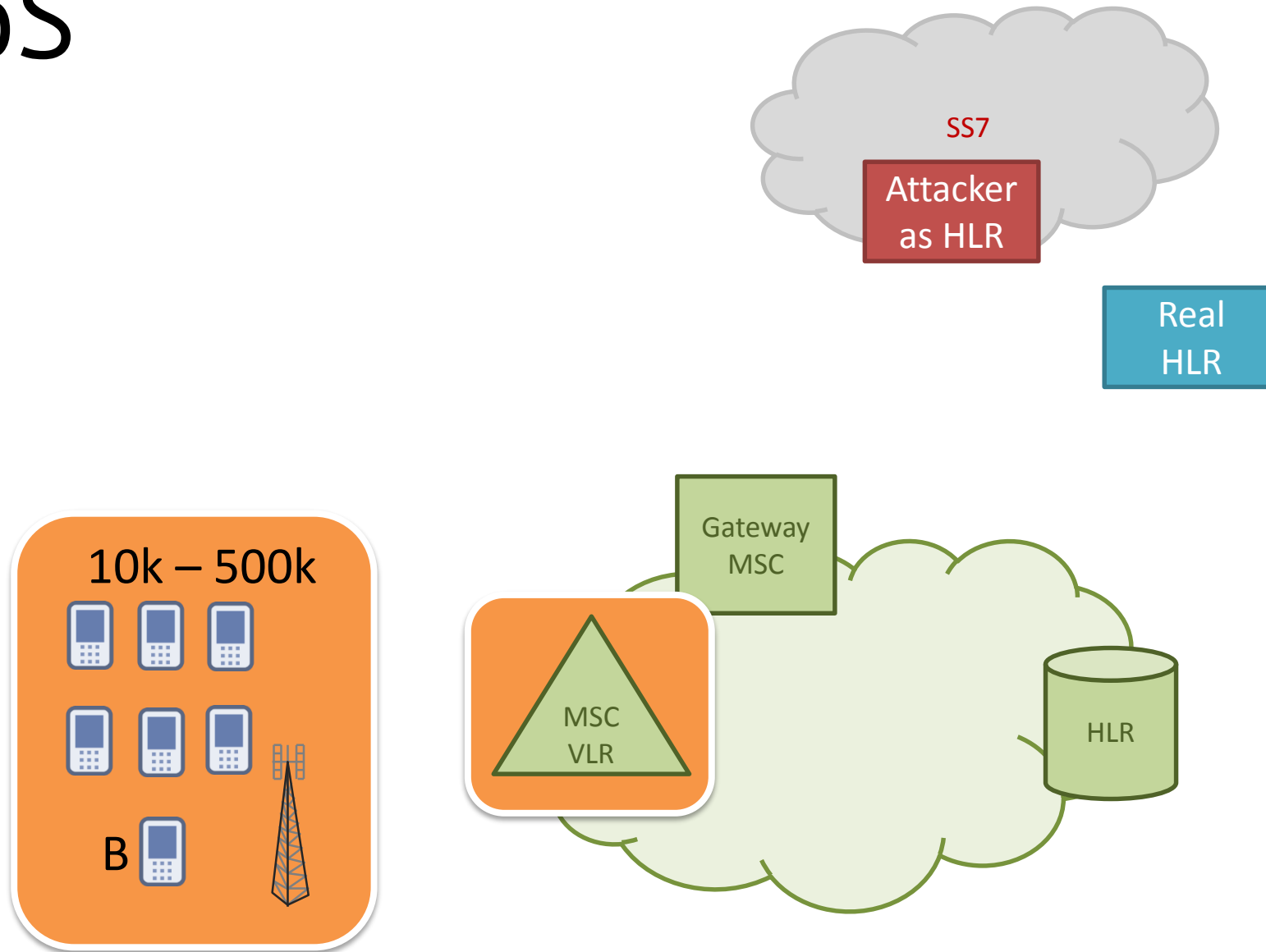
...

MSRN 0 123 4569999

noRoamingNumberAvailable

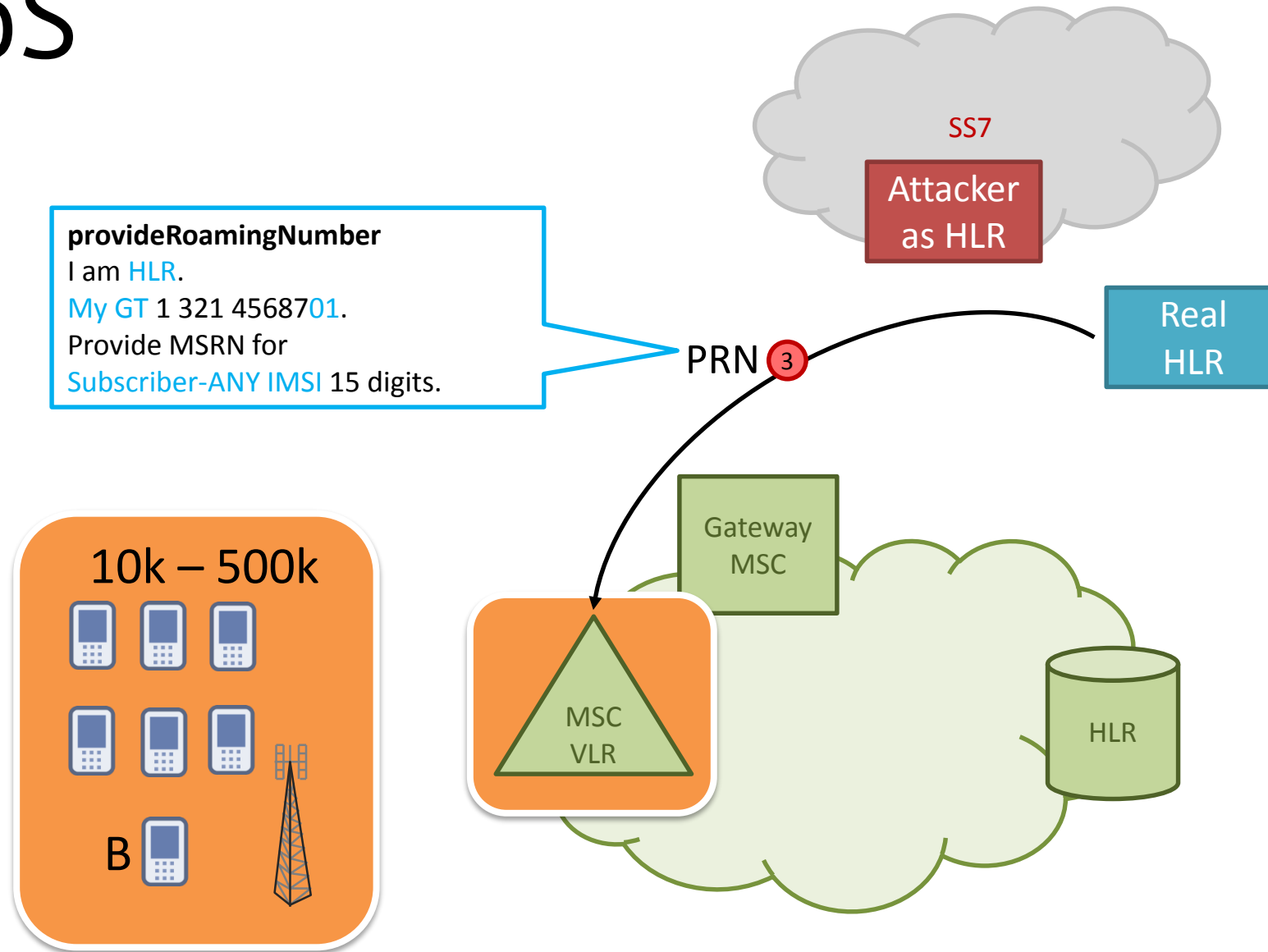
HLR

# DoS

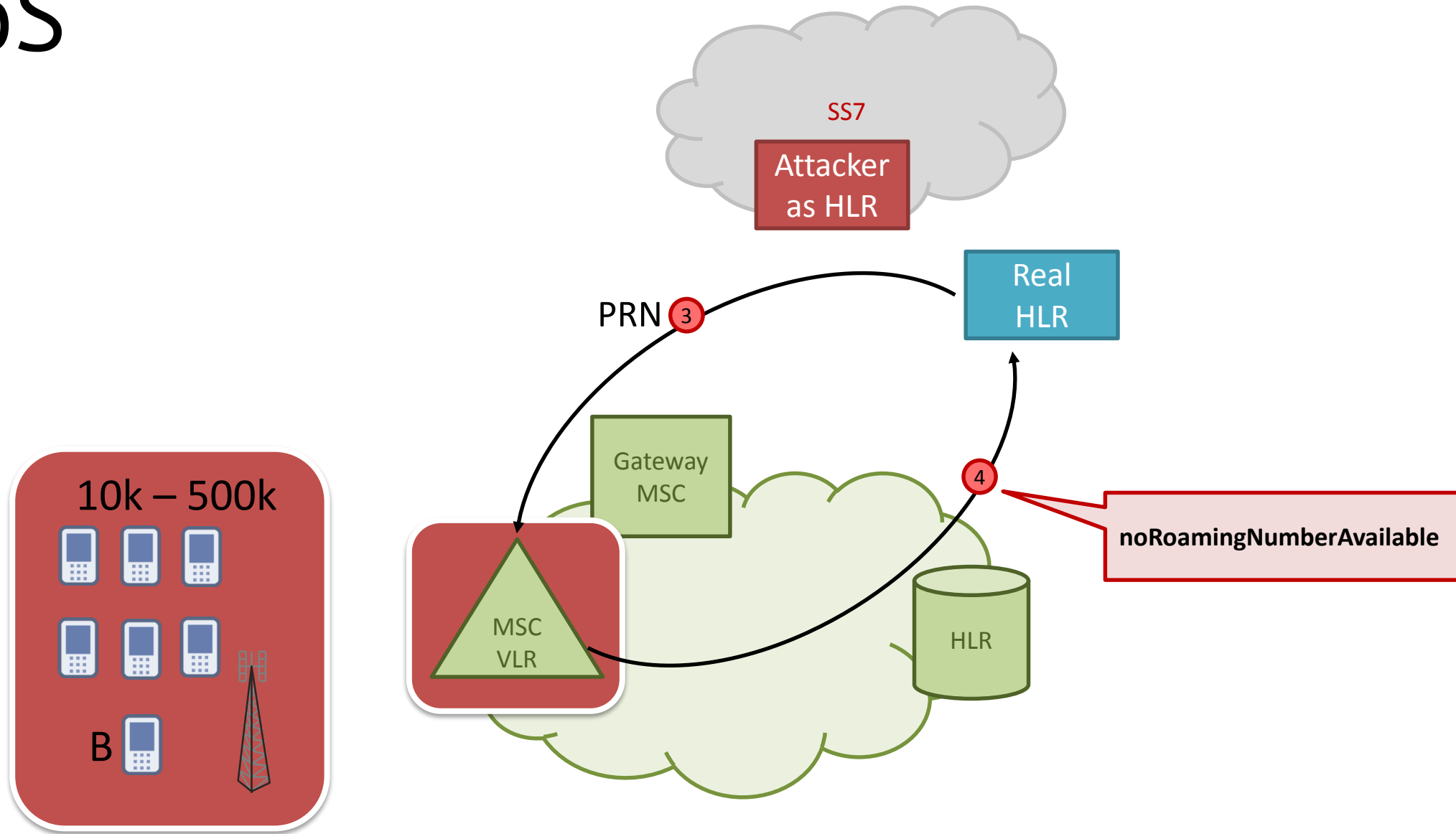




# DoS

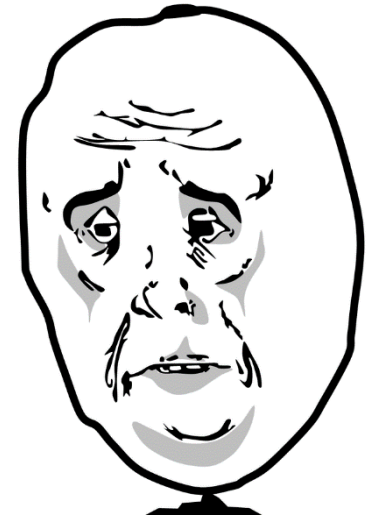
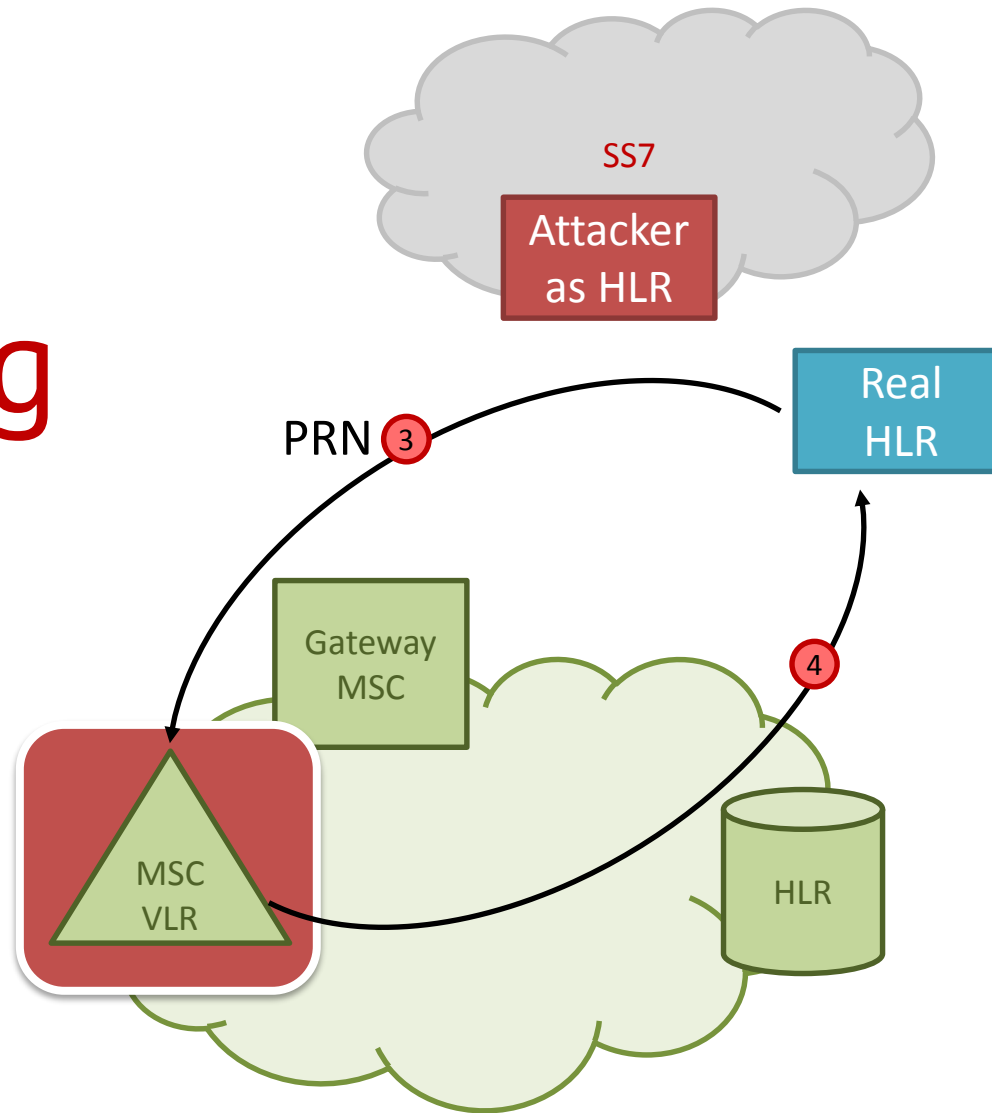
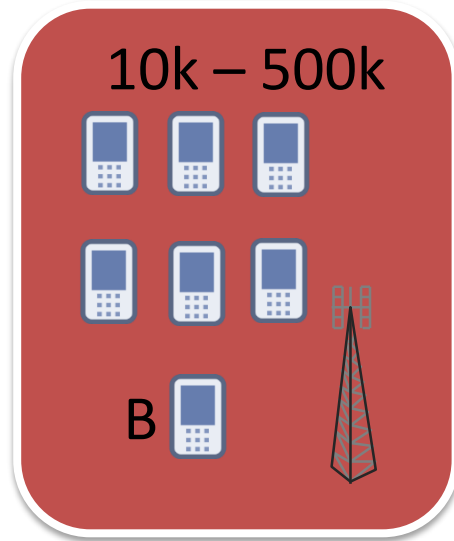


# DoS



# DoS

## No incoming calls

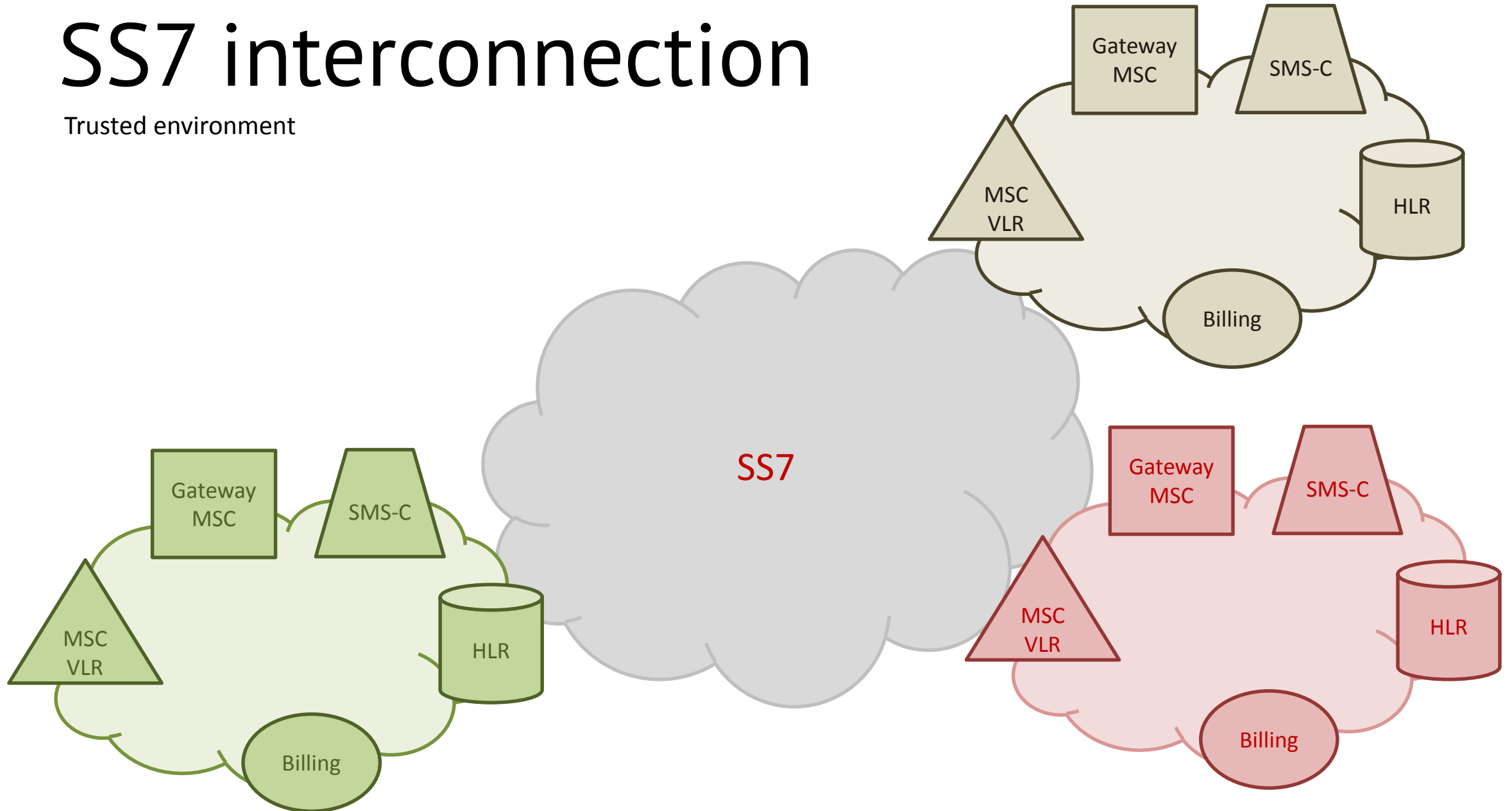


Sad calling party

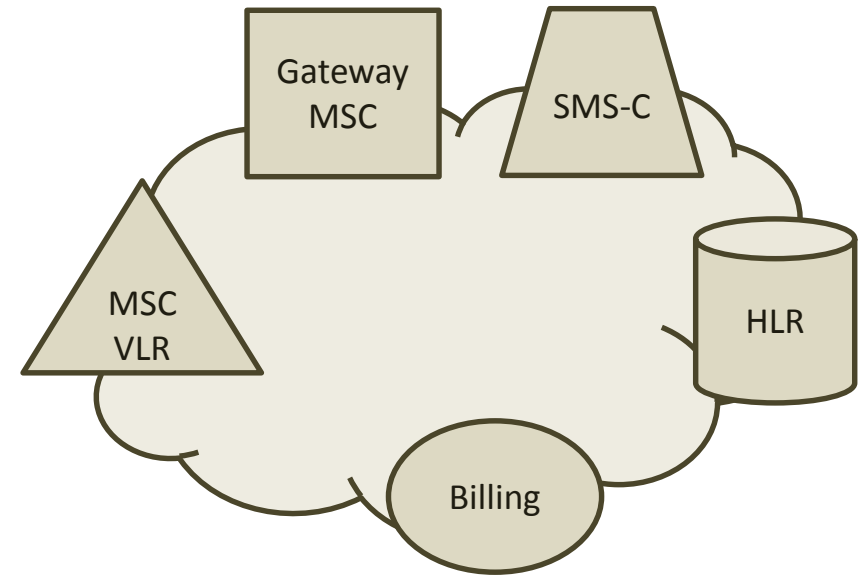
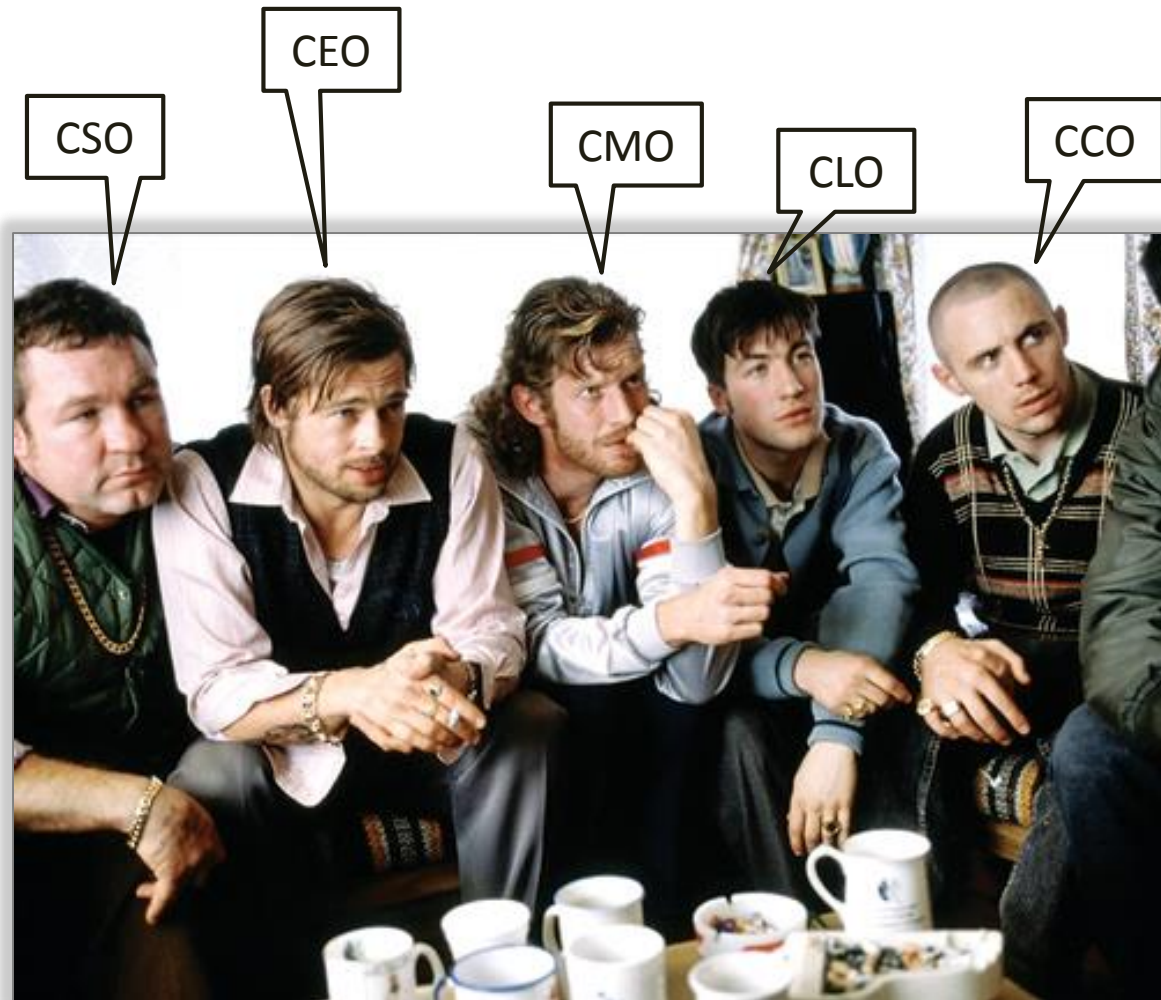
# Fraud in SS7

# SS7 interconnection

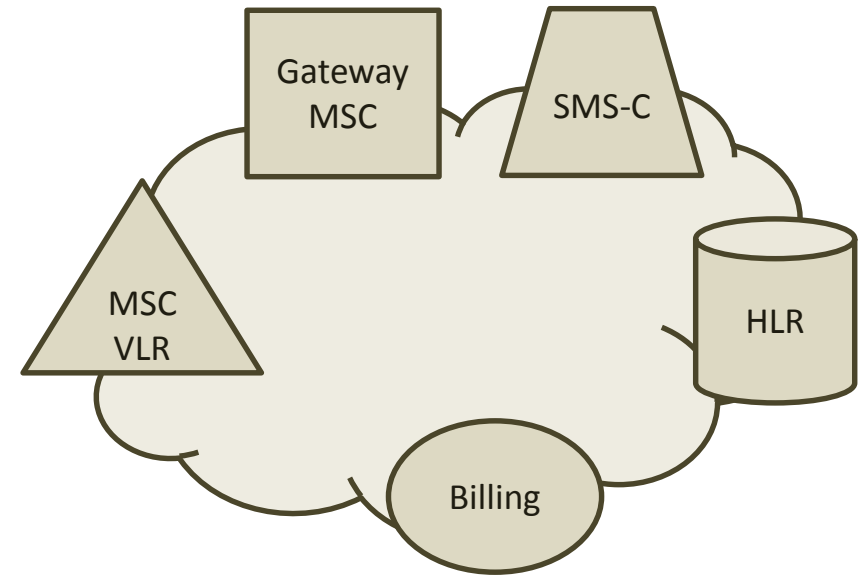
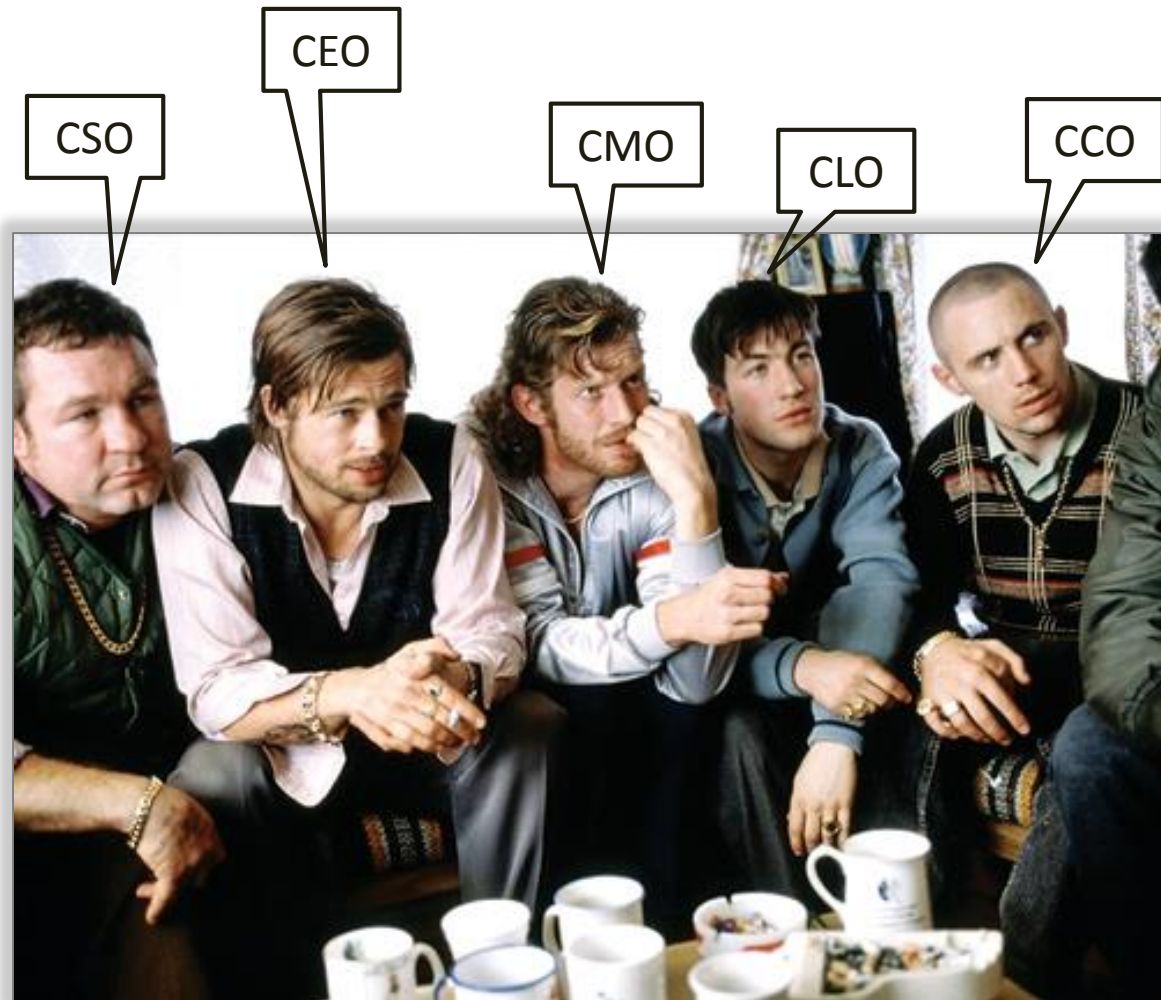
Trusted environment



# Leadership team



# Leadership team

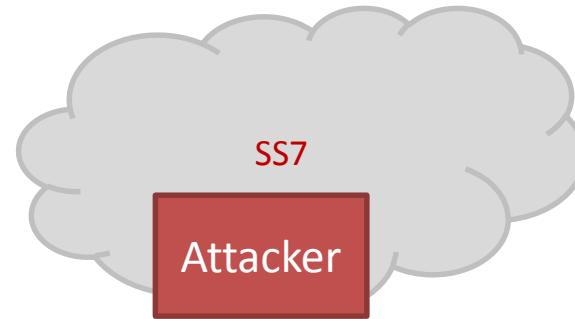


Really?!  
Trust them?

# Uncharged calls

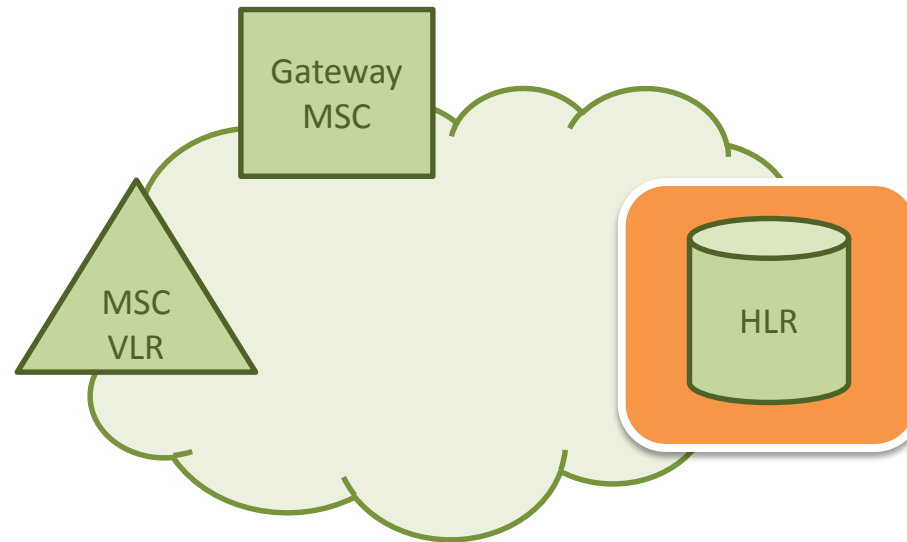
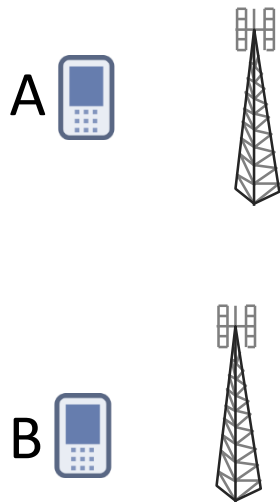


# Collect info

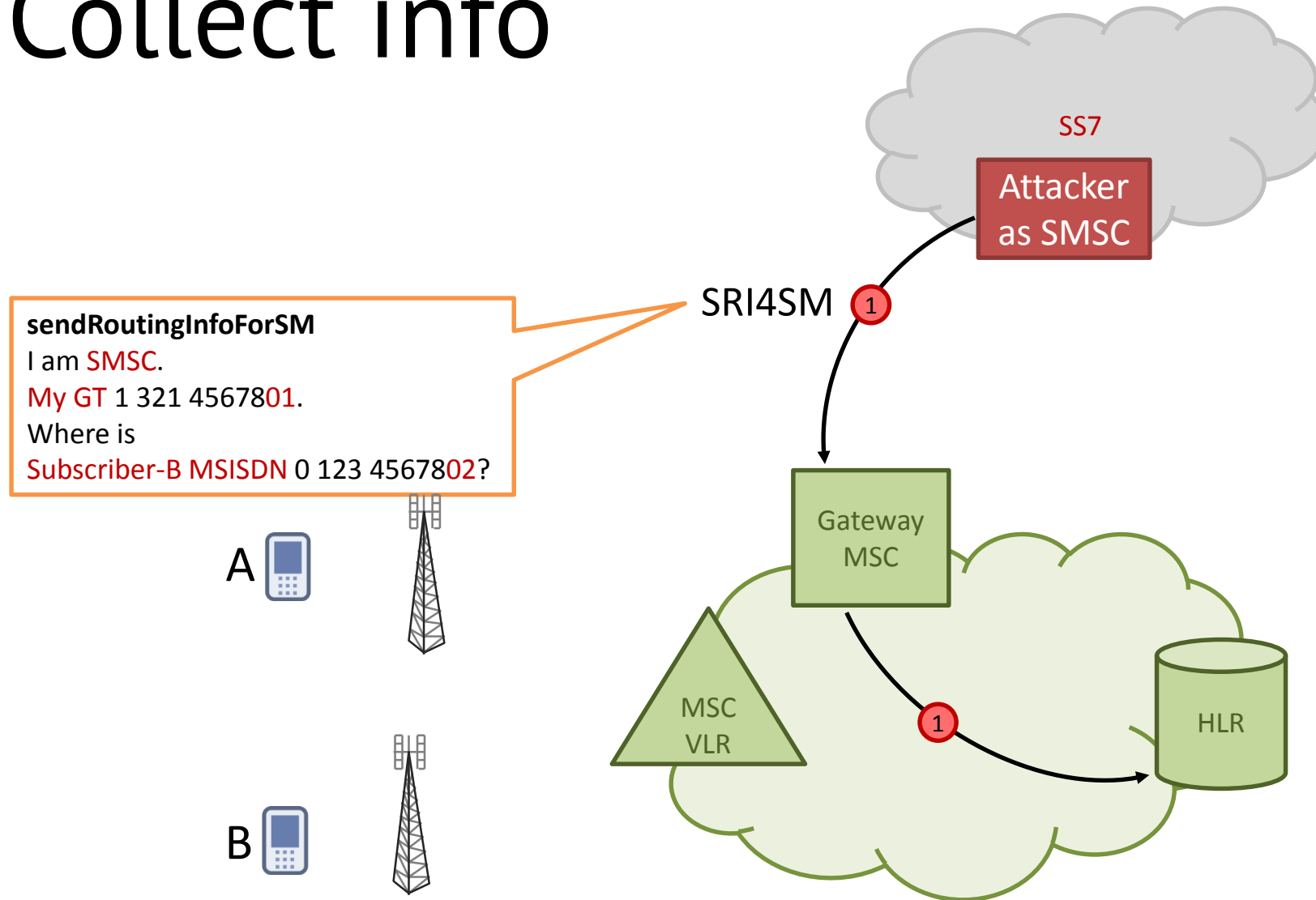


We know

**B-Number** 0 123 45678**02**



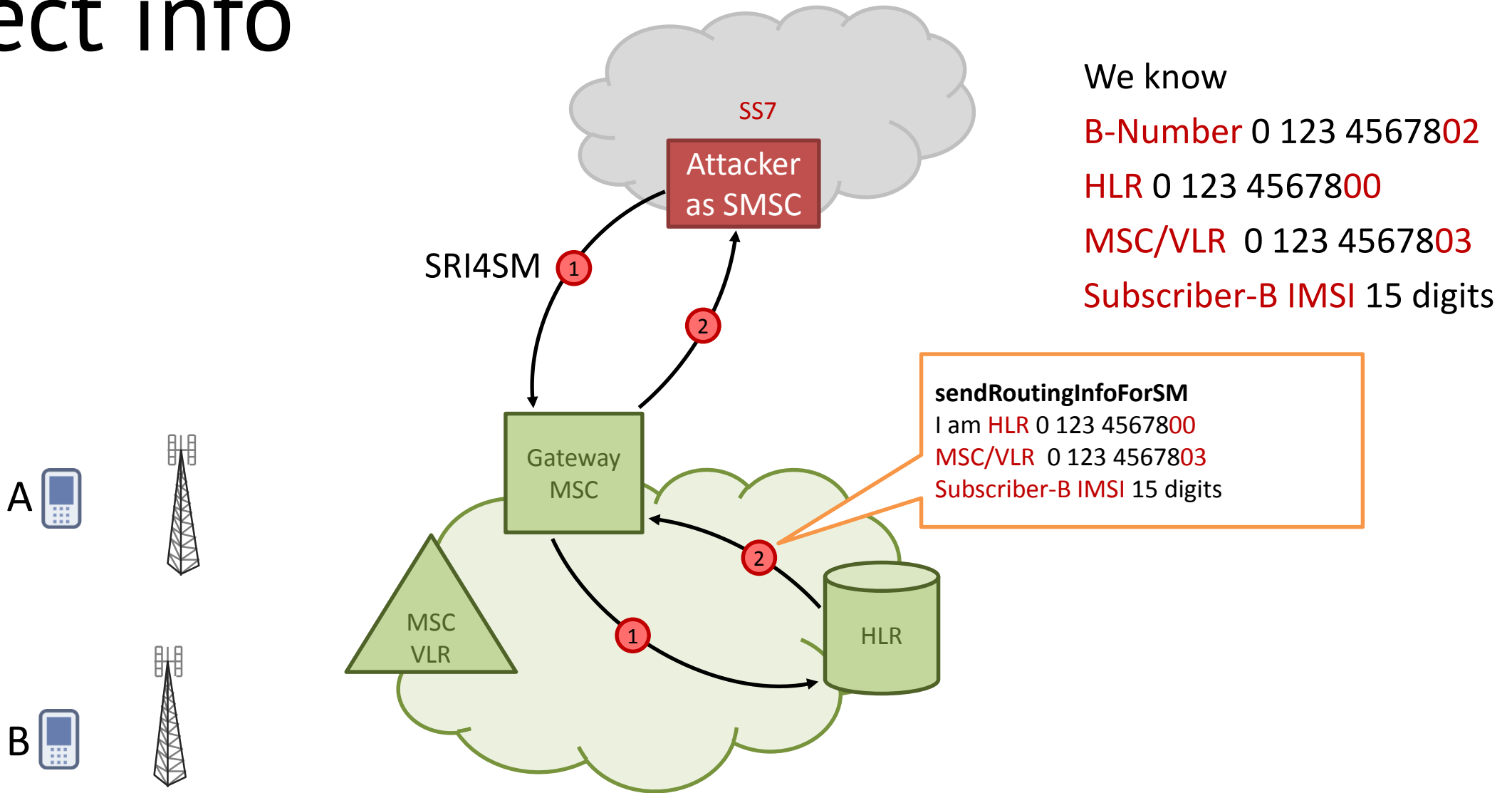
# Collect info



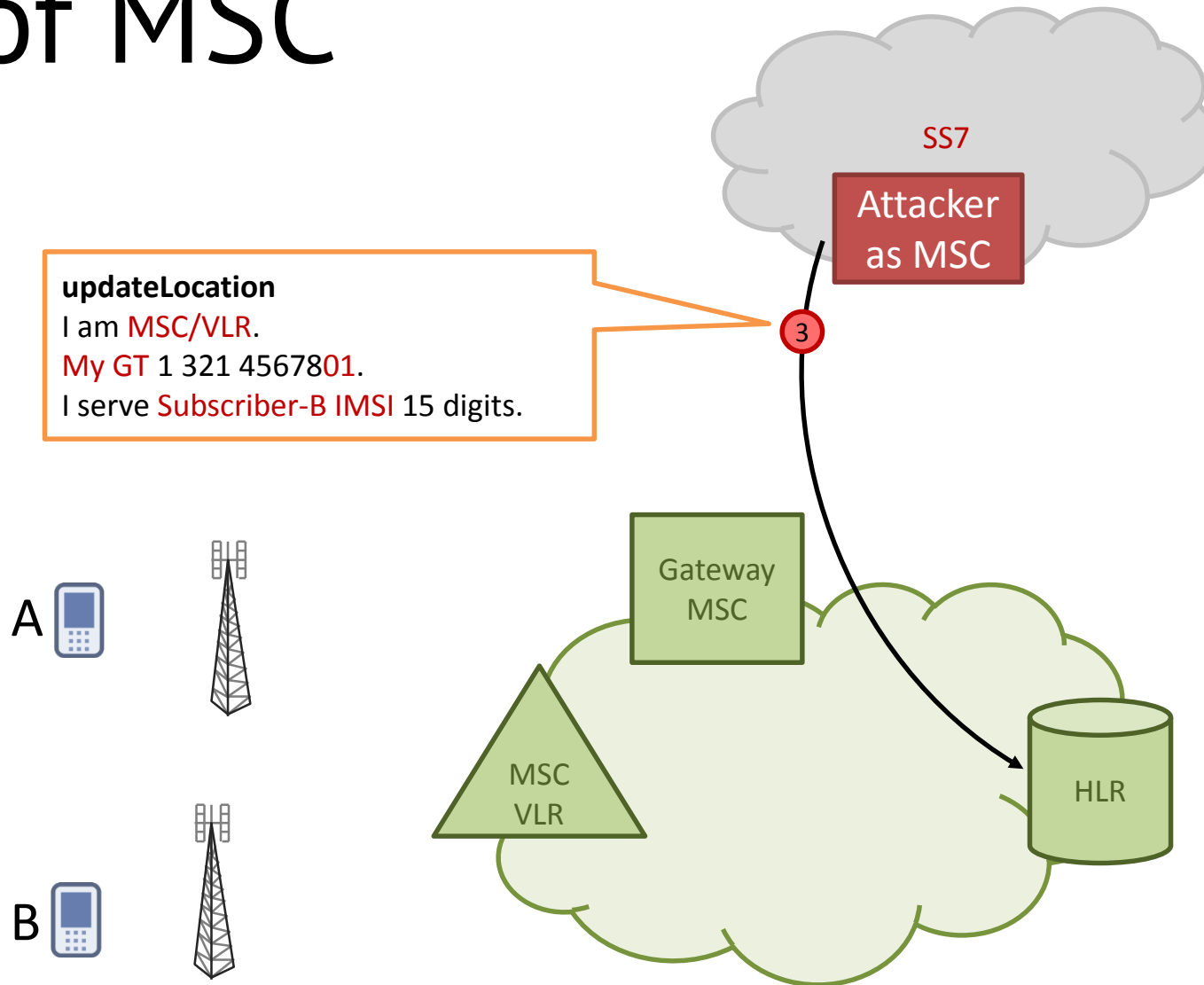
We know

**B-Number** 0 123 4567802

# Collect info



# Spoof MSC

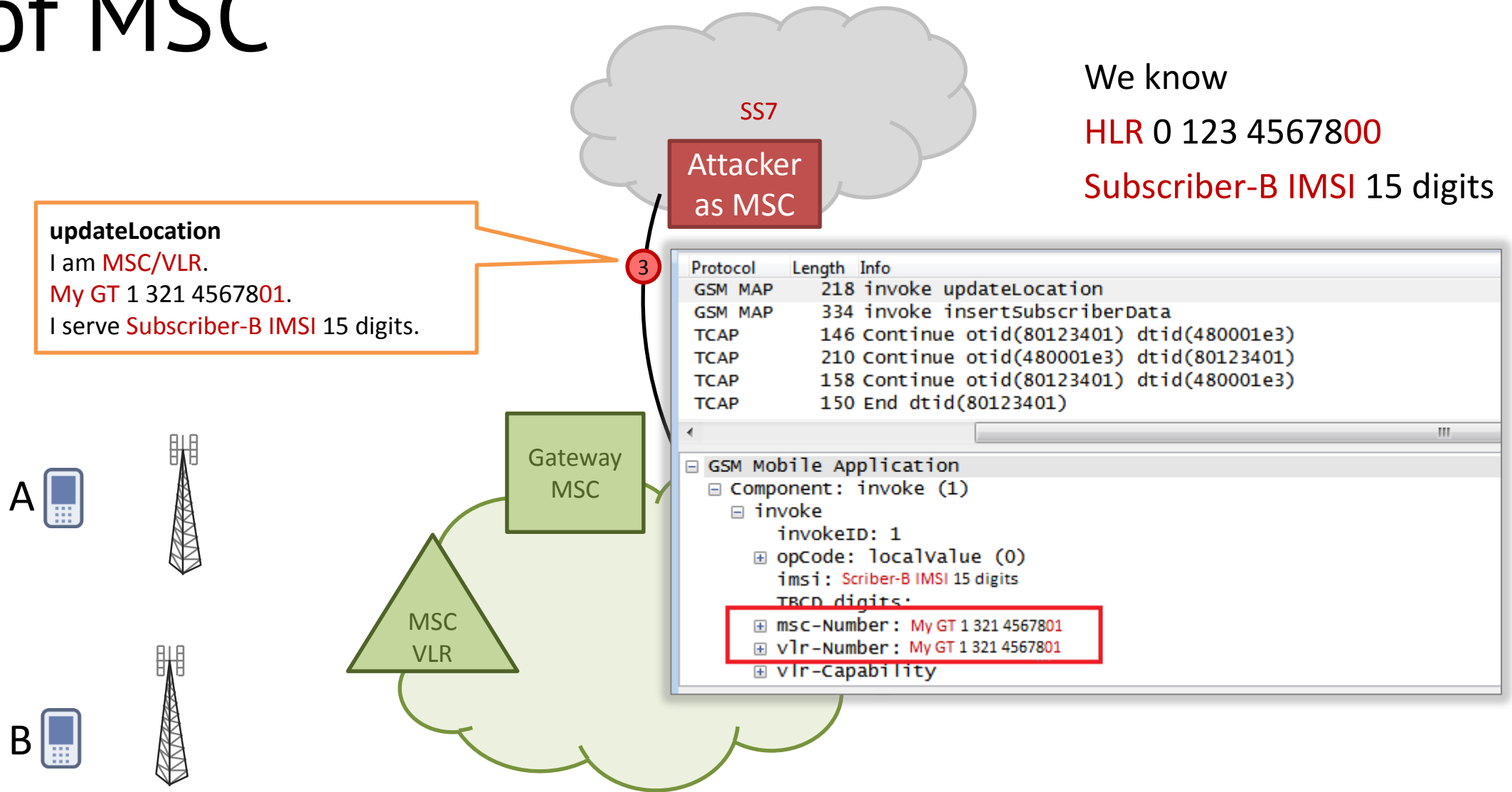


We know

**HLR 0 123 4567800**

**Subscriber-B IMSI 15 digits**

# Spoof MSC



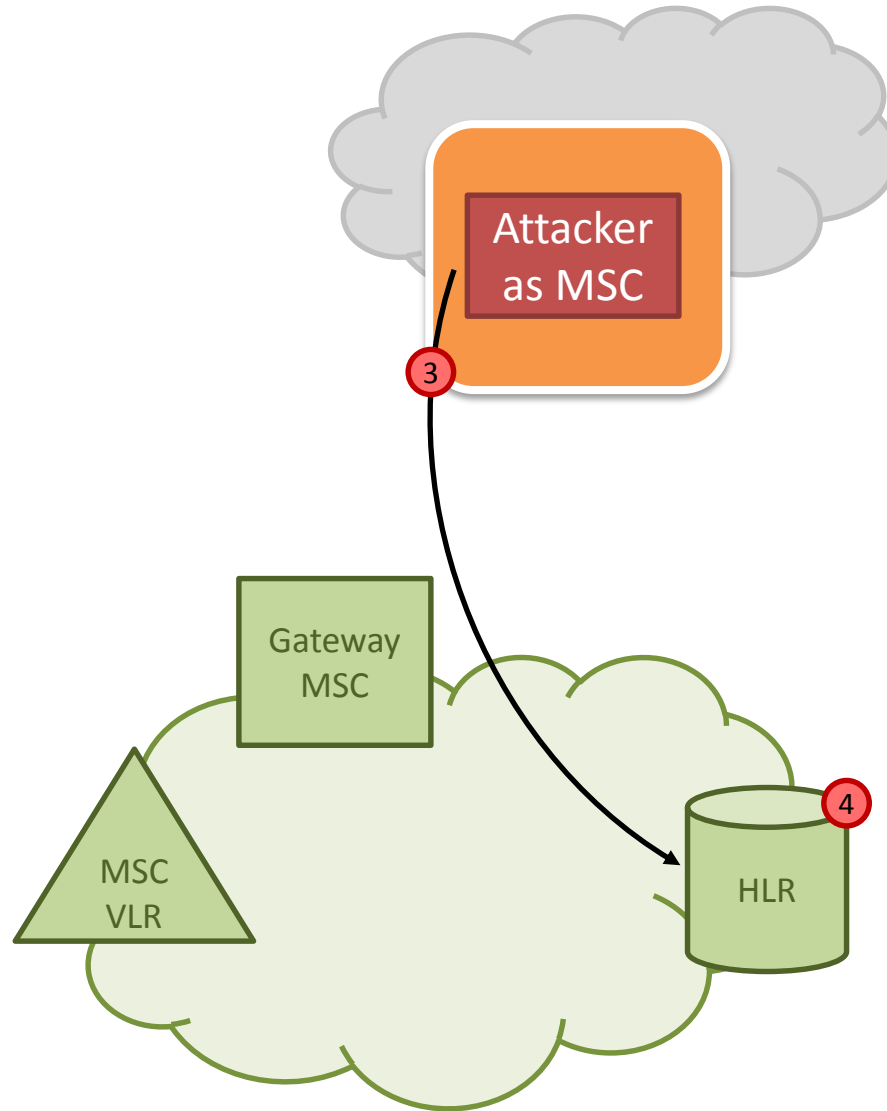
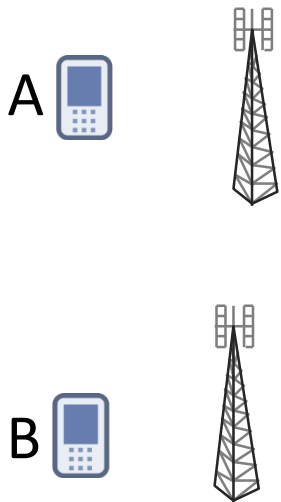
We know

**HLR 0 123 4567800**

**Subscriber-B IMSI 15 digits**

# Spoof MSC

Attacker serves  
Subscriber-B



We know

HLR 0 123 4567800

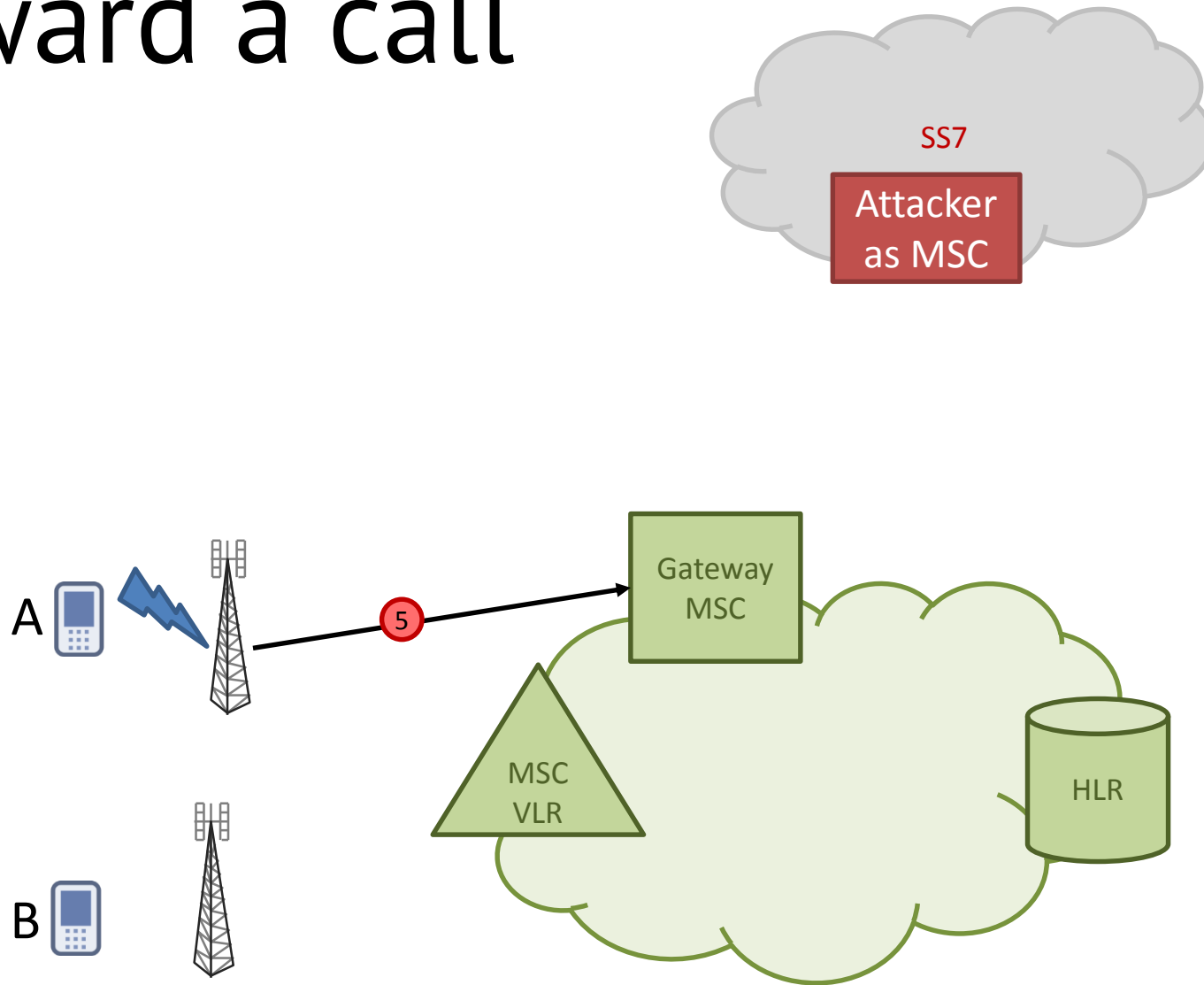
Subscriber-B IMSI 15 digits

HLR stores

Subscriber-B IMSI 15 digits

MSC/VLR 1 321 4567801

# Forward a call



HLR stores

Subscriber-B

MSISDN 0 123 4567802

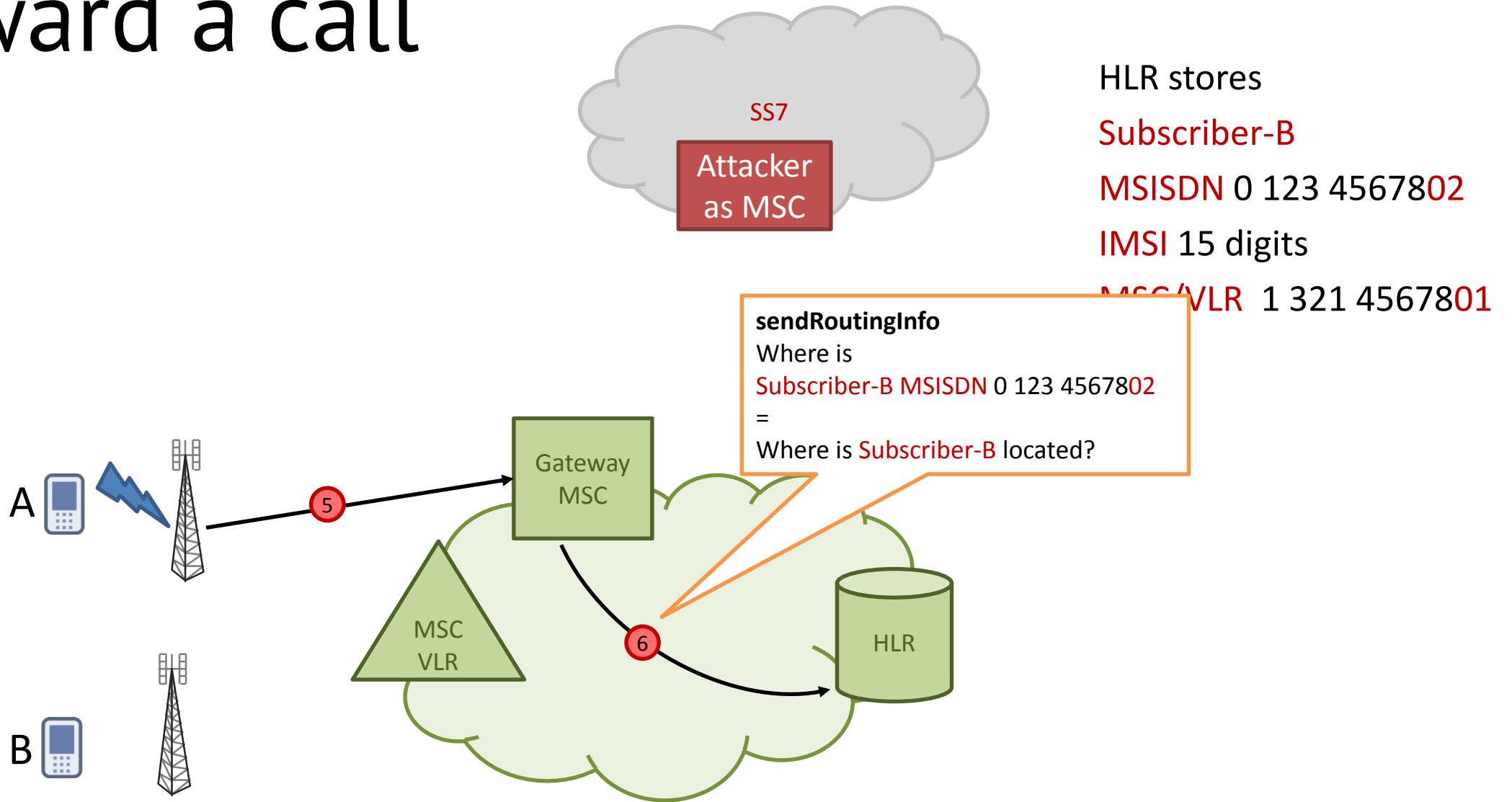
IMSI 15 digits

MSC/VLR 1 321 4567801

GatewayMSC knows

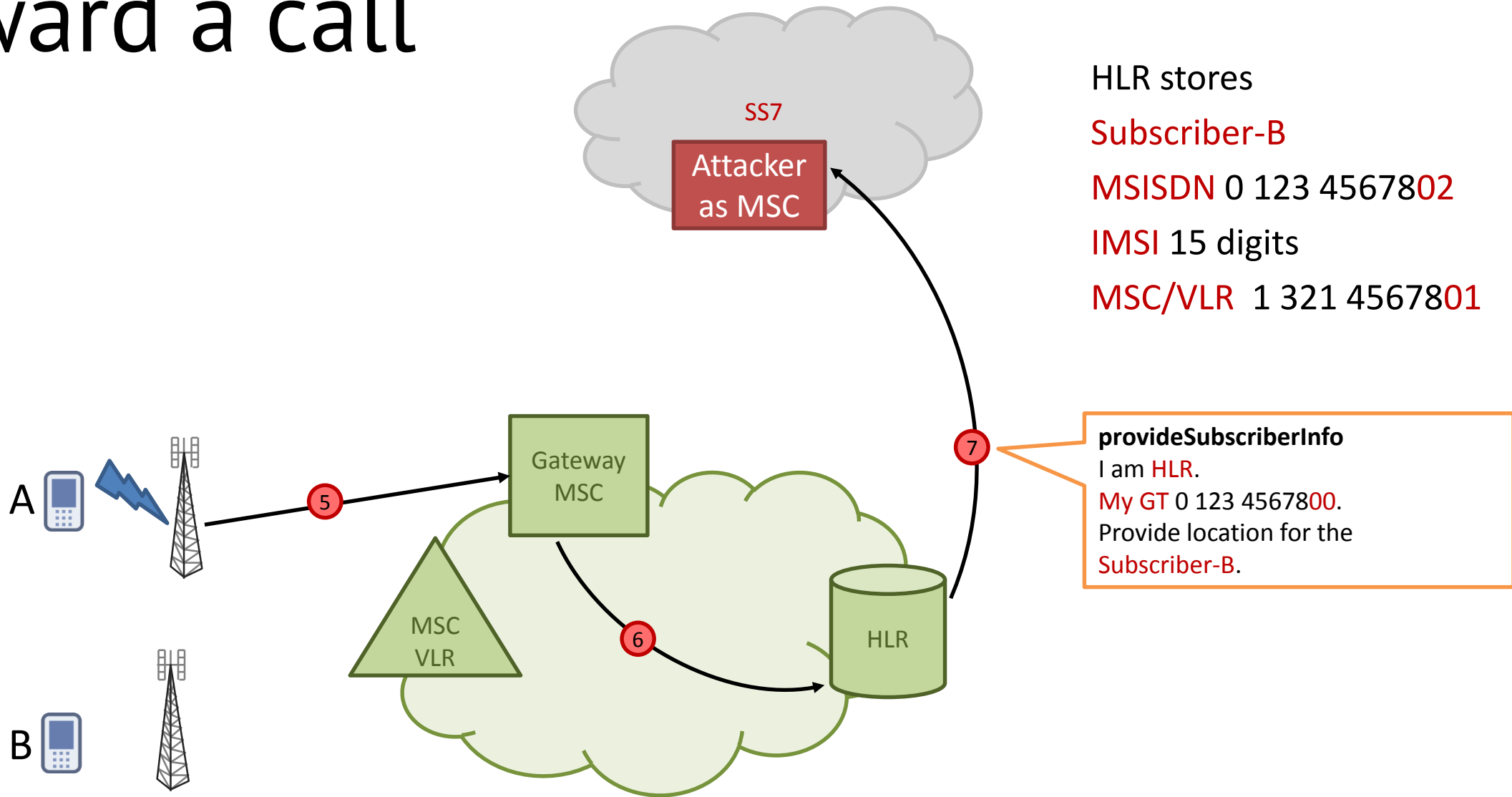
nothing

# Forward a call

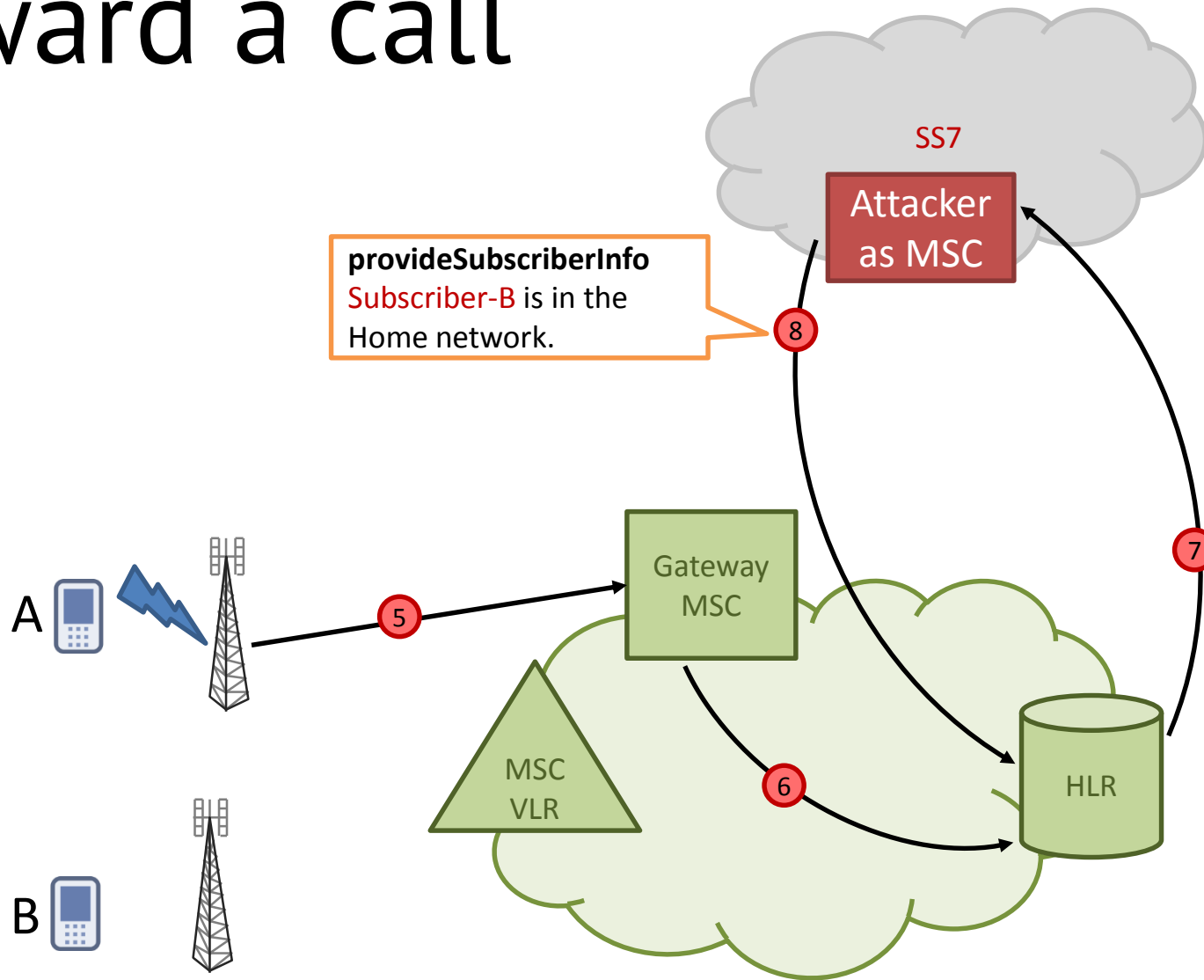




# Forward a call



# Forward a call



HLR stores

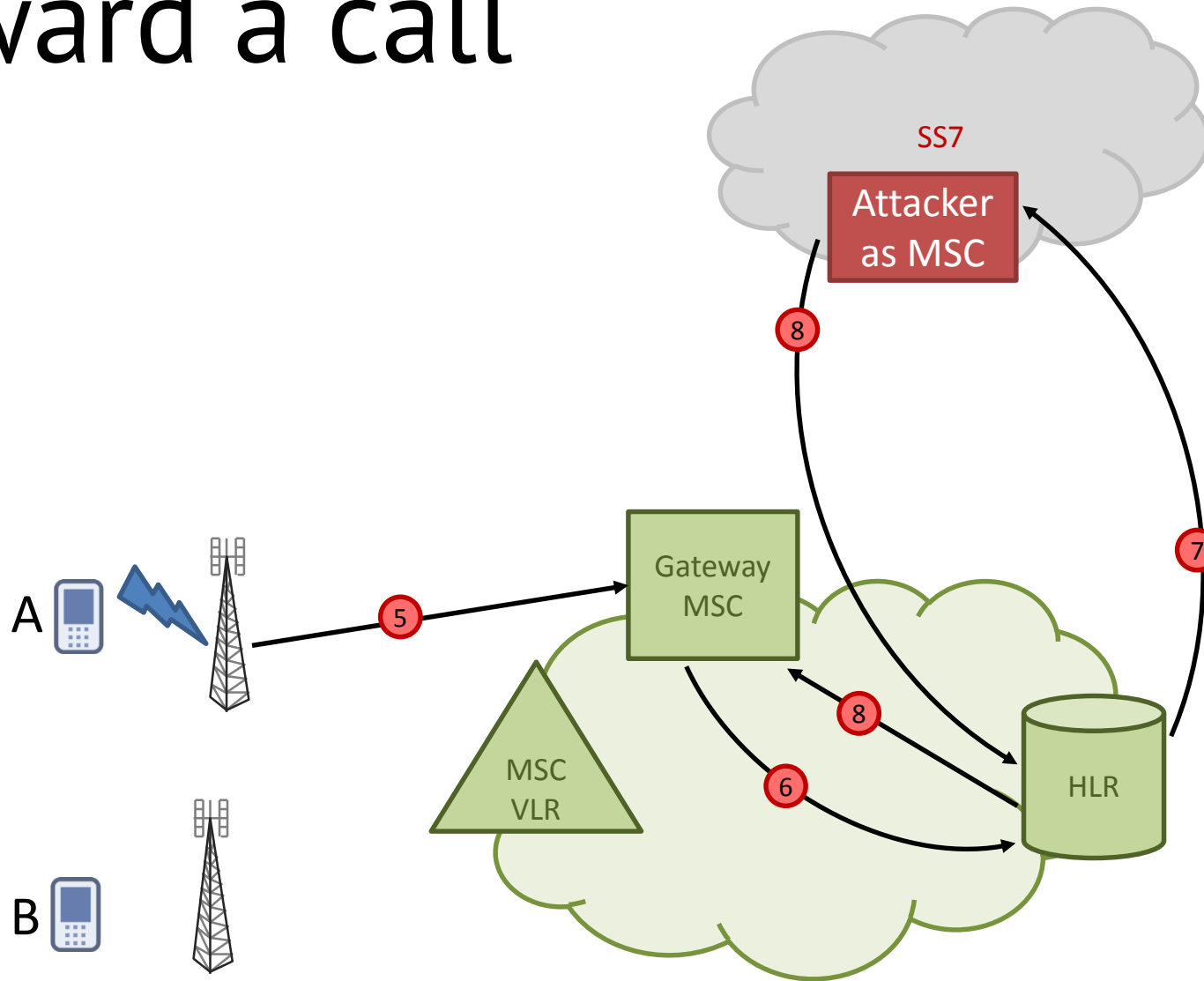
Subscriber-B

MSISDN 0 123 4567802

IMSI 15 digits

MSC/VLR 1 321 4567801

# Forward a call



HLR stores

Subscriber-B

MSISDN 0 123 4567802

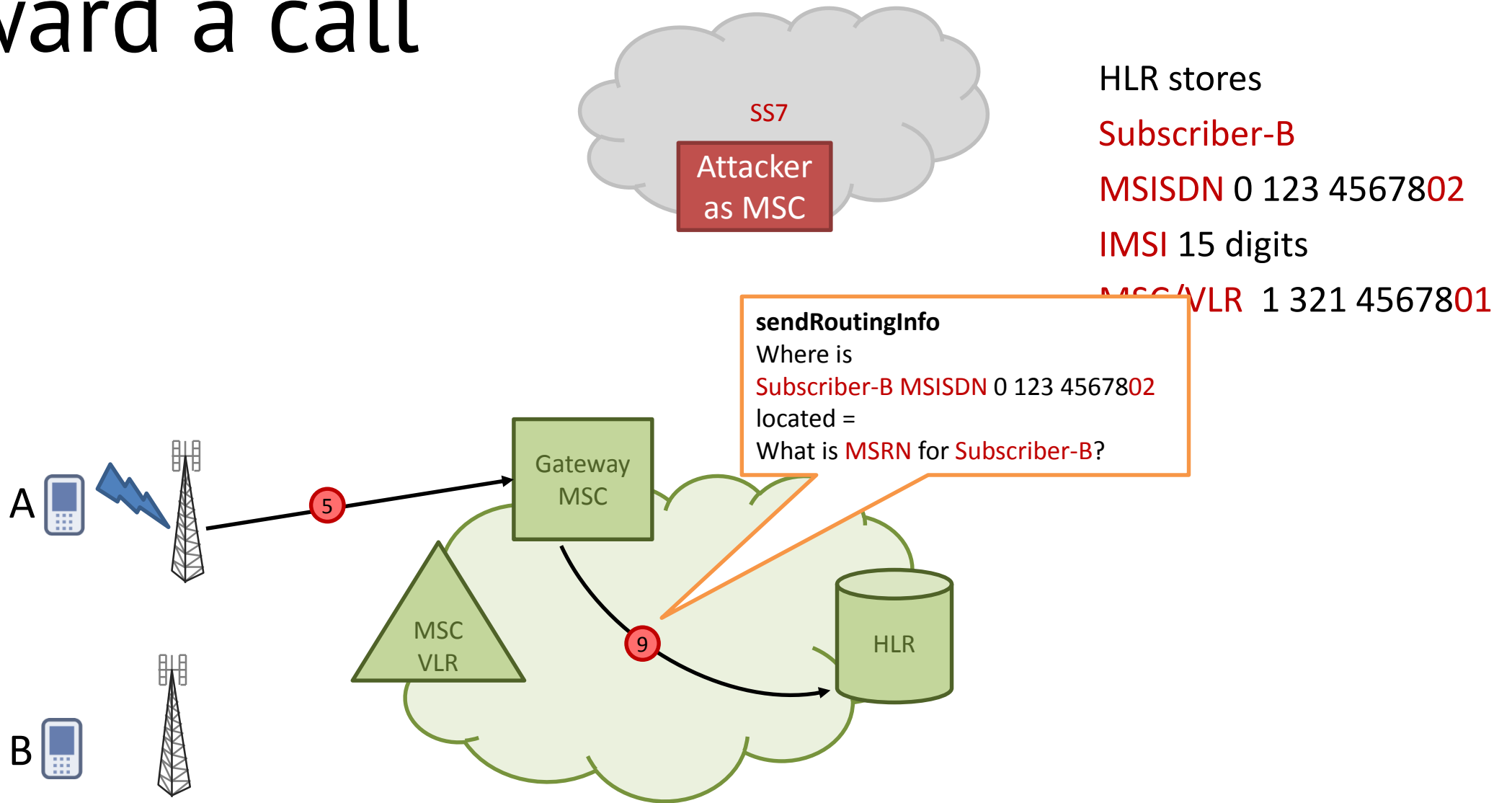
IMSI 15 digits

MSC/VLR 1 321 4567801

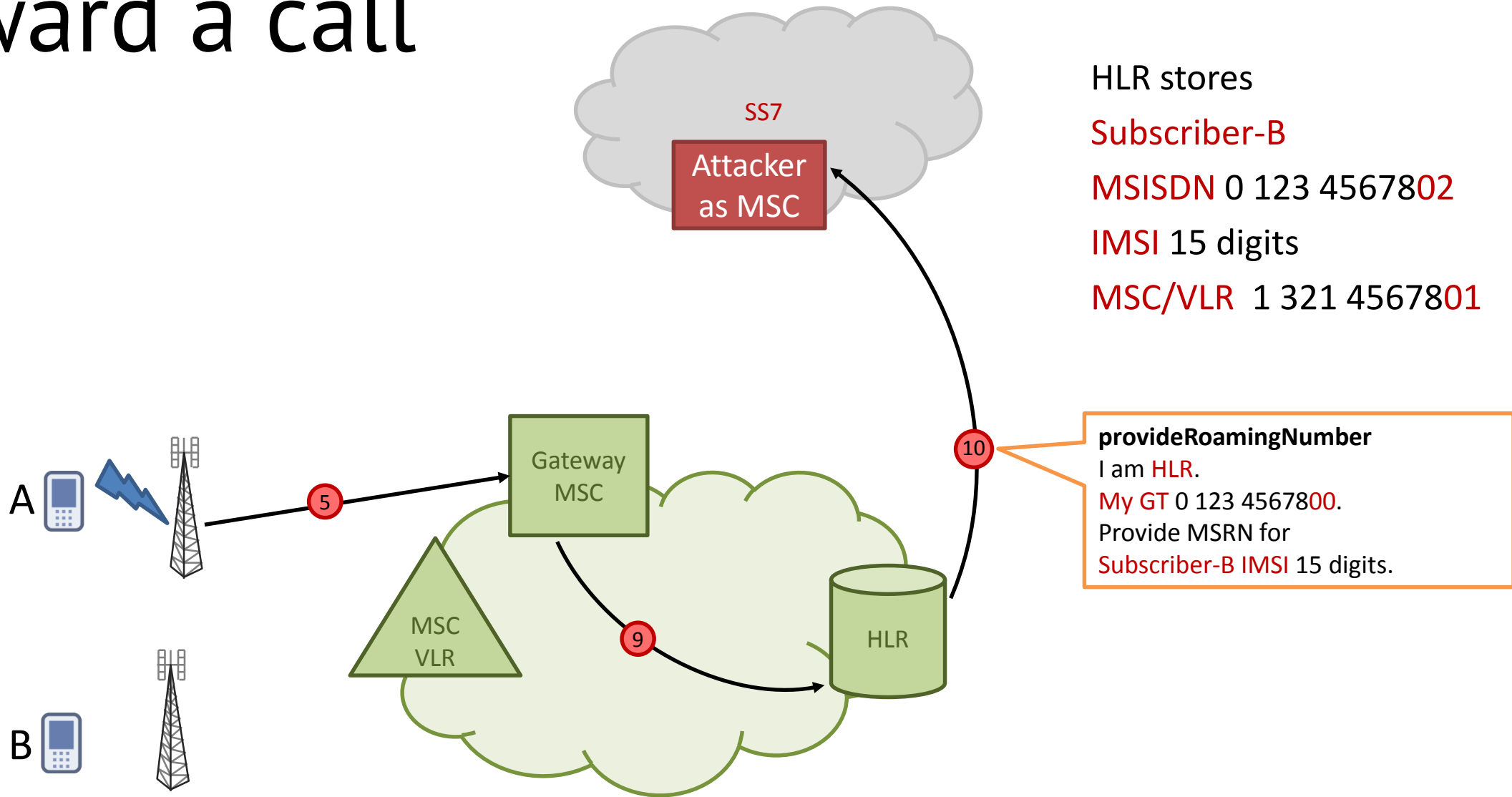
GatewayMSC knows that  
Subscriber-B is at home.

This information will be  
sent to a billing platform.

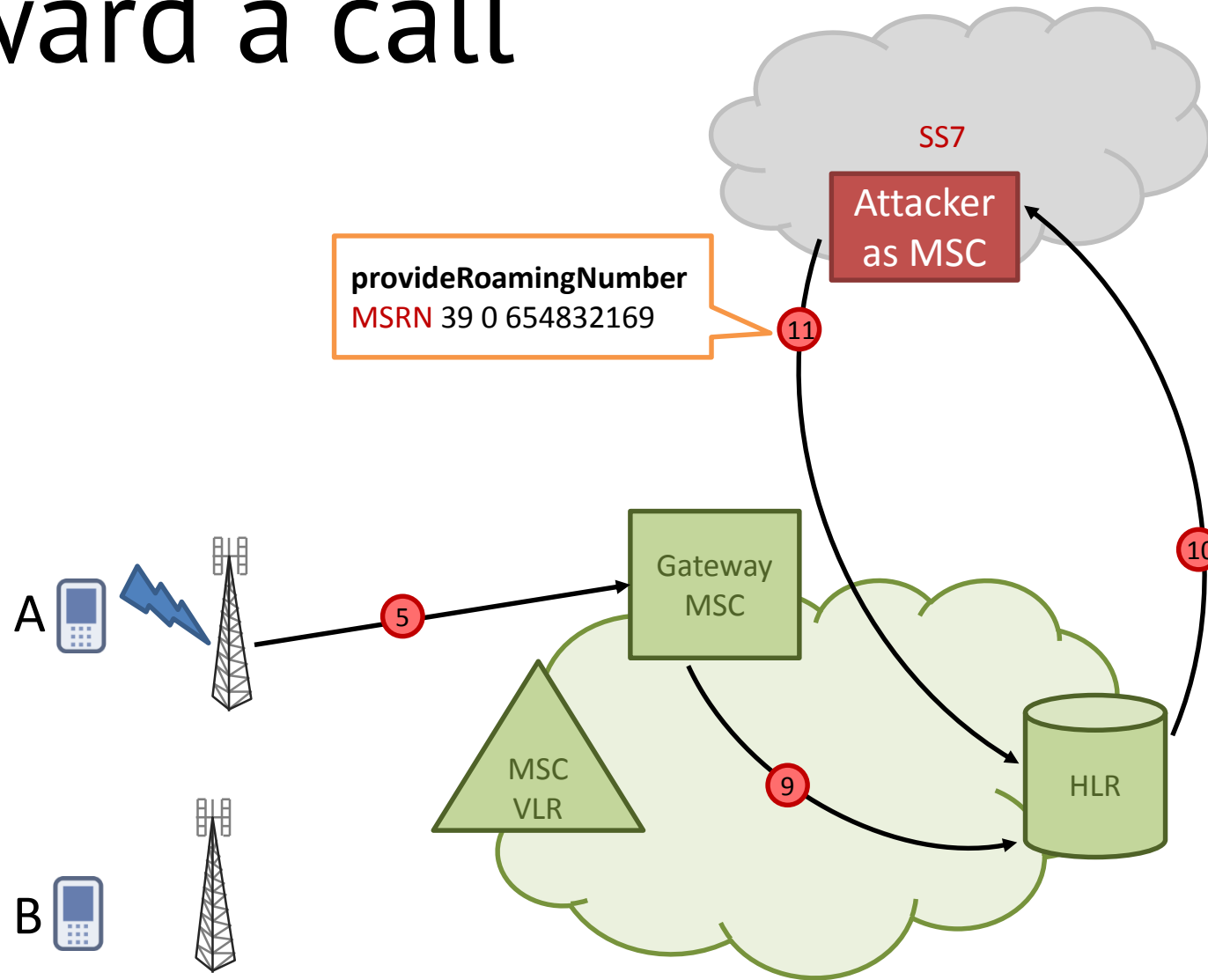
# Forward a call



# Forward a call



# Forward a call



HLR stores

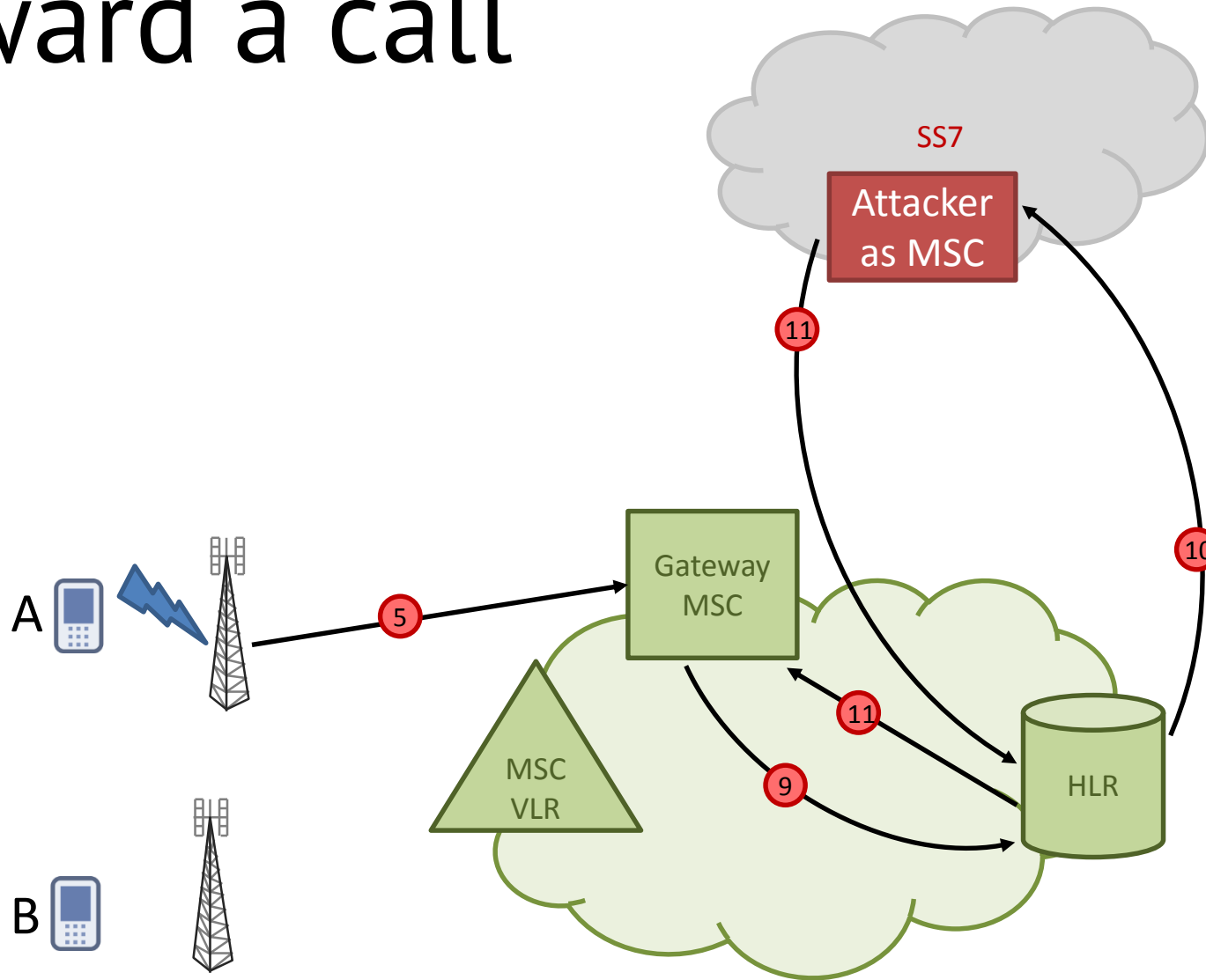
Subscriber-B

MSISDN 0 123 4567802

IMSI 15 digits

MSC/VLR 1 321 4567801

# Forward a call



HLR stores

Subscriber-B

MSISDN 0 123 4567802

IMSI 15 digits

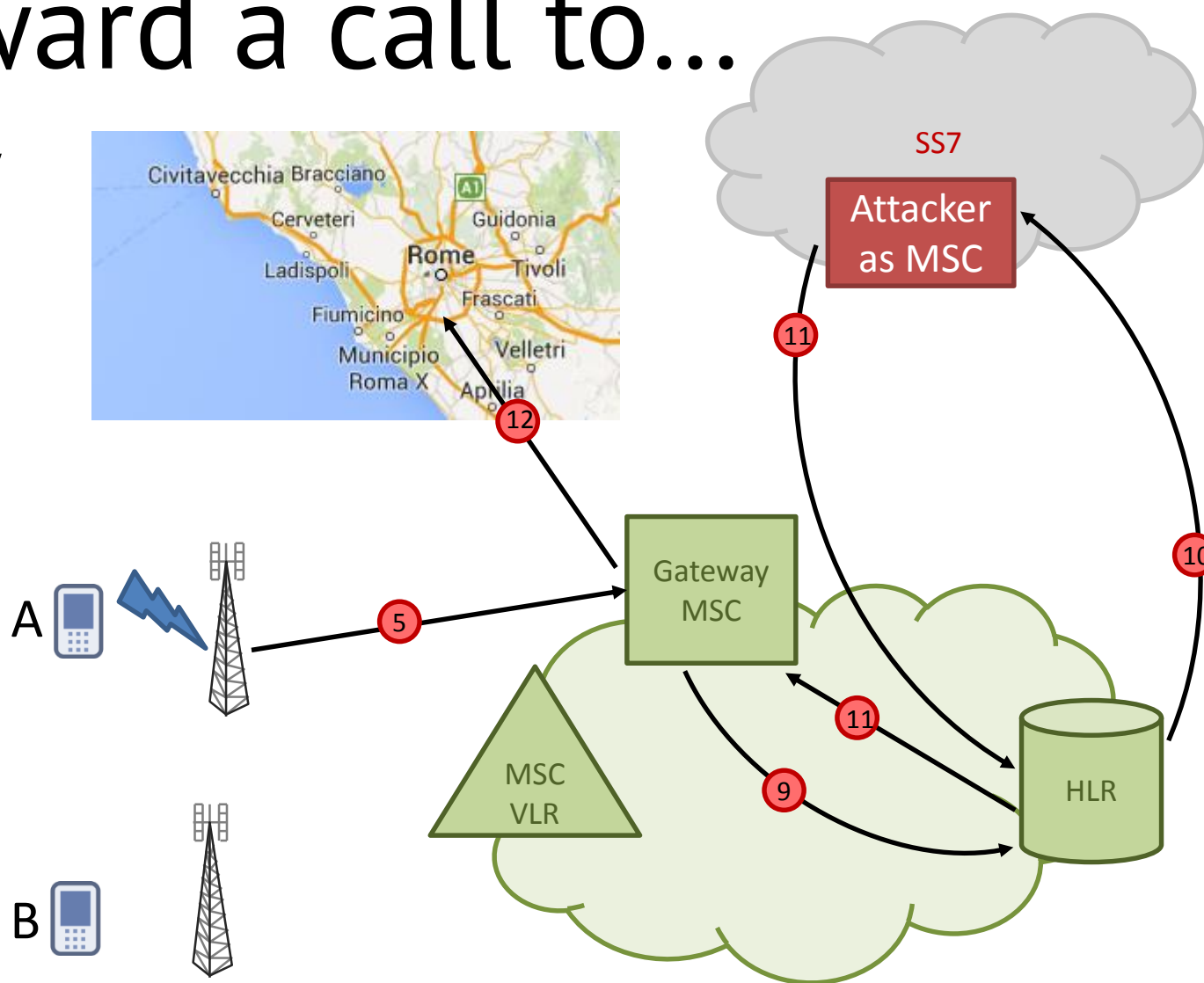
MSC/VLR 1 321 4567801

GatewayMSC knows

Subscriber-B

MSRN 39 0 654832169

# Forward a call to... Italy



HLR stores

Subscriber-B

MSISDN 0 123 4567802

IMSI 15 digits

MSC/VLR 1 321 4567801

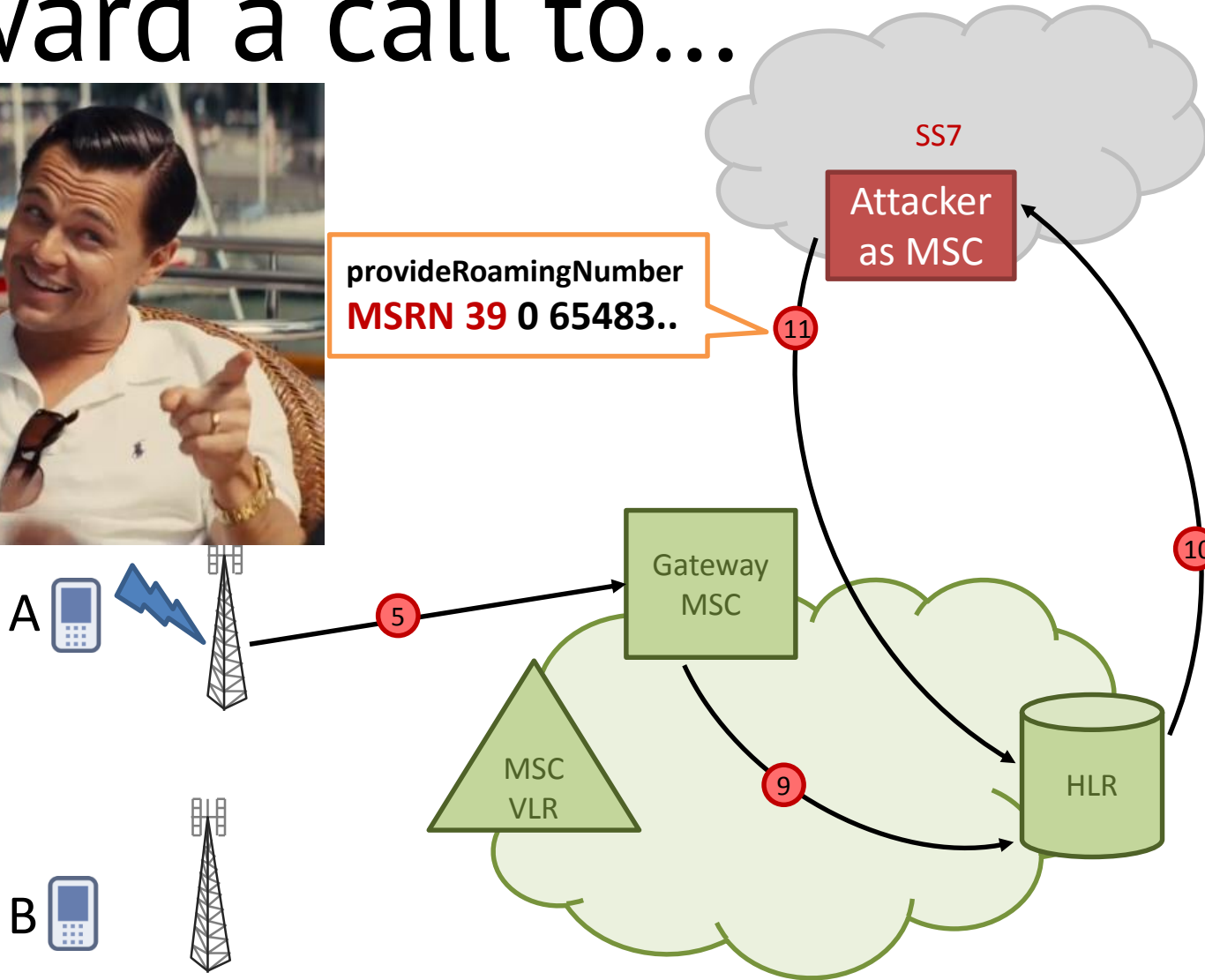
GatewayMSC knows

Subscriber-B

MSRN 39 0 654832169



# Forward a call to...



HLR stores

Subscriber-B

MSISDN 0 123 4567802

IMSI 15 digits

MSC/VLR 1 321 4567801

GatewayMSC knows

Subscriber-B

MSRN 39 0 654832169

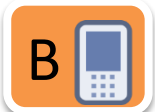
# Demo

# Who pays?

Call from  to  while at “home” = ₺ 1,60

Call from  to  = ₺ 30,00

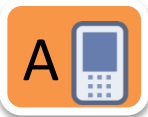
# Who pays?

Call from  to  while at “home” = ₺ 1,60

Call from  to  = ₺ 30,00

**₺ 30,00 - ₺ 1,60 = ₺ 28,40** – Attacker profit

# Who pays?

Call from  A to  B while at “home” = ₺ 1,60

Call from  A to  Italy = ₺ 30,00

International calls  
on 5,3% of original price

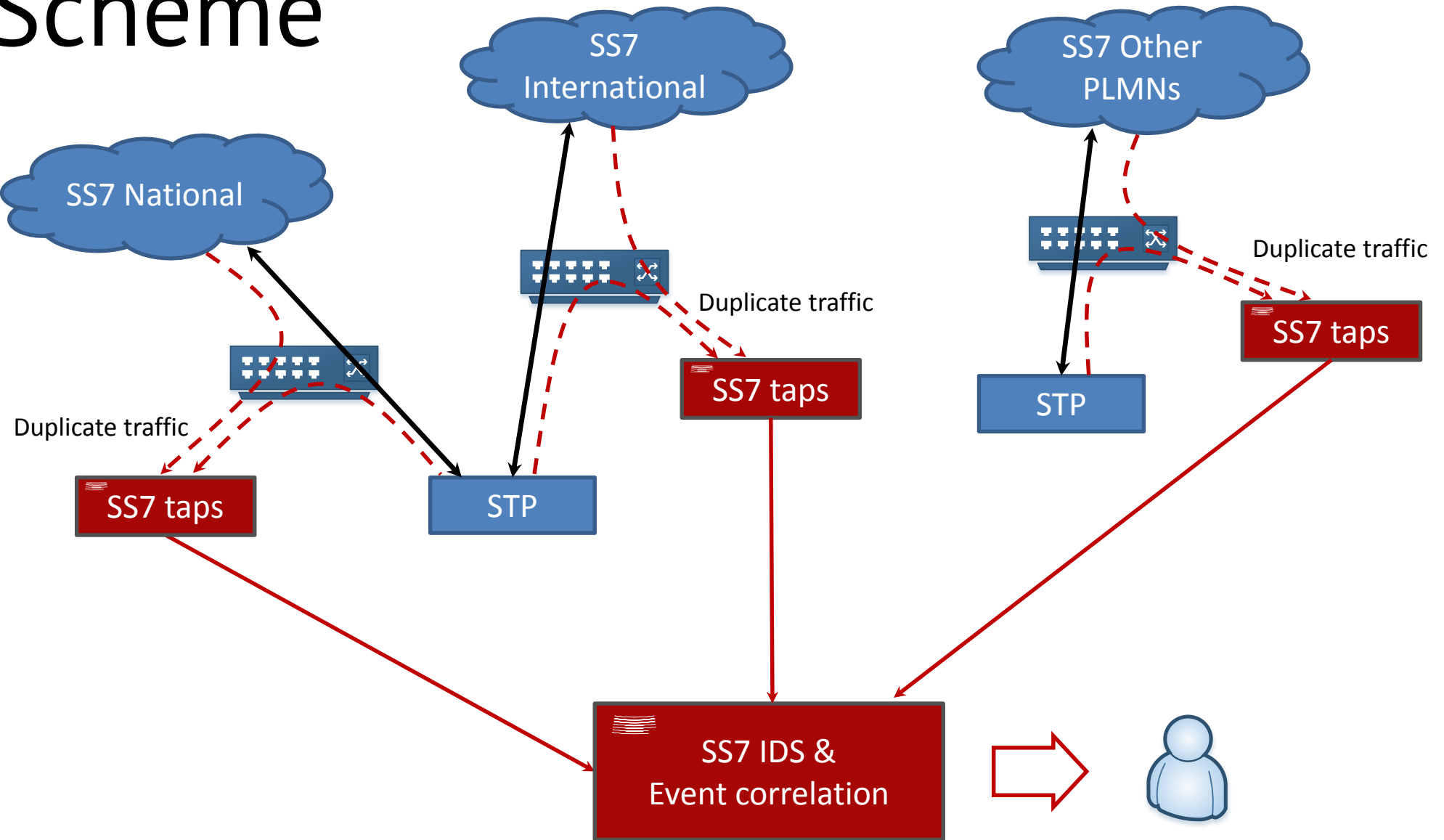
₺ 30,00 - ₺ 1,60 = ₺ 28,40 – Attacker’s profit

How much does a mobile operator lose?

To Do:

SS7 Firewall or IDS with evolution to  
IPS?

# IDS Scheme



# Research Updates

- SS7 security threats
- Mobile Internet vulnerabilities (GPRS)
- SIM vulnerabilities

[www.ptsecurity.com](http://www.ptsecurity.com)

<http://blog.ptsecurity.com/>





# Questions?

Dmitry Kurbatov

[dkurbatov@ptsecurity.com](mailto:dkurbatov@ptsecurity.com)